Innominate mGuard delta

Benutzerhandbuch

Software-Release 3.1.0

Innominate Security Technologies AG
Albert-Einstein-Str. 14
D-12489 Berlin
Tel.: +49 (0)800-366 4666
info@innominate.com
www.innominate.com

© Innominate Security Technologies AG

Dezember 2005
„Innominate“ und „mGuard“ sind registrierte Handelsnamen der Innominate Security Technologies AG. Die mGuard Technologie ist durch die Patent 10138865 und 10305413, erteilt durch das Deutschen Patentamt, geschützt. Weitere Patente sind angemeldet.
Weder das Gesamtdokument noch Teile davon dürfen ohne schriftliche Genehmigung übertragen oder kopiert werden.
Die Innominate AG behält sich das Recht vor, jederzeit und ohne Benachrichtigung dieses Dokument zu verändern. Innominate übernimmt keine Gewährleistung für diese Unterlagen. Dies gilt ohne Einschränkung auch für die stillschweigende Zusicherung der Verkäuflichkeit und der Eignung für einen bestimmten Zweck.
Innominate übernimmt ferner keine Haftung für Fehler im vorliegenden Handbuch sowie für zufällige oder Folgeschäden im Zusammenhang mit der Lieferung, Leistung oder Verwendung dieser Unterlagen.
Ohne die vorherige schriftliche Zustimmung der Innominate Security Technologies AG darf dieses Handbuch weder teilweise noch vollständig fotokopiert, vervielfältigt oder in eine andere Sprache übersetzt werden.

Innominate Dokumentennummer: 513108-173

Inhalt

1 Einleitung ... 4
Netzwerk-Features ... 4
Firewall-Features ... 4
Anti-Virus-Features ... 4
VPN-Features ... 4
Weitere Features ... 4
Support ... 5
2 Typische Anwendungsszenarien ... 6
Stealthmodus ... 6
Netzwerkrouter ... 6
DMZ ... 6
VPN Gateway ... 7
WLAN über VPN ... 7
3 Bedienelemente und Anzeigen ... 9
4 Inbetriebnahme ... 10
4.1 Lieferumfang ... 10
5 Konfiguration ... 11
Voraussetzungen ... 11
5.1 Lokale Konfiguration: Bei Inbetriebnahme ... 11
Erster Zugriff auf den mGuard ... 11
5.2 Lokale Konfigurationsverbindung herstellen ... 12
Web-basierte Administratoroberfläche ... 12
Bei erfolgreichem Verbindungsaufbau ... 13
Konfiguration durchführen ... 14
5.3 Fernkonfiguration ... 14
Voraussetzung ... 14
Fernkonfiguration durchführen ... 14
5.4 Arbeiten mit Tabellen ... 15
Einfügen von Zeilen ... 15
Verschieben von Zeilen ... 15
Löschen von Zeilen ... 15
5.5 Startseite ... 16
5.6 Menü Netzwerk ... 16
Netzwerk → Basis ... 16
Netzwerk → Stealth ... 19
Netzwerk → Router ... 20
Netzwerk → PPPoE ... 21
Netzwerk → PPTP ... 22
Netzwerk → MAU Konfiguration ... 23
Netzwerk → Erweiterte Einstellungen ... 23
Netzwerk → Status ... 24
5.7 Menü Firewall ... 25
Firewall → Eingehend ... 25
Firewall → Ausgehend ... 26
Firewall → Port Weiterleitung ... 27
Firewall → NAT ... 29
Firewall → 1:1 NAT ... 29
Firewall → MAC Filter ... 30
Firewall → Erweiterte Einstellungen ... 31
Firewall → Logs ... 33
5.8 Menü Antivirus ... 34
Kaspersky Engine ... 34

Unterstützte Kompressionsformate 34
Voraussetzungen zur Nutzung 34
Ablauf der Antivirus-Lizenz 34
Dateigrößen-begrenzung 34
Antivirus → SMTP-Einstellungen 35
Antivirus → POP3-Einstellungen 37
Antivirus → HTTP-Einstellungen 40
Antivirus → FTP-Einstellungen 42
Antivirus → Datenbank-Update 44
Antivirus → Antivirus Status 46
Antivirus → Lizenzanforderung 46
Antivirus → Lizenzdatei installieren 47
Antivirus → Virus Logs 47
Antivirus → Update Logs 48
5.9 Menü VPN (nur enterprise) 49
VPN → Verbindungen 49
Weitere IKE Einstellungen 55
VPN → Maschinenzertifikat 57
VPN → IPsec Status 59
VPN → L2TP Status 60
VPN → VPN Logs 60
5.10 Menü Dienste 61
Dienste → DNS 61
Dienste → DynDNS Überwachung 62
Dienste → DynDNS Registrierung 62
Dienste → DHCP Intern/Extern 64
Dienste → LLDP 66
Dienste → Redundanz (nur mGuard enterprise XL) 67
Dienste → Remote Logging 69
Dienste → SNMP Traps 69
5.11 Menü Zugang 71
Zugang → Passworte 71
Zugang → Sprache 72
Zugang → HTTPS 72
Zugang → SSH 74
Zugang → SNMP 75
Zugang → Serieller Port/Modem 77
5.12 Menü Eigenschaften 79
Eigenschaften → Lokales Update 79
Eigenschaften → Online Update 79
Eigenschaften → Installiere Lizenz 80
Features → Softwareinformation 80
Eigenschaften → Lizenzinformation 81
Eigenschaften → Hardwareinformation 81
5.13 Menü Support 82
Support → Snapshot 82
Support → Status 82
5.14 Menü System 84
Dienste → Systemzeit 84
System → Konfigurationsprofile 85
System → Konfiguration holen 86
System → Neustart 87
System → Logs 88
5.15 CIDR (Classless InterDomain Routing) 89

Inhalt

5.16 Netzwerk-Beispielskizze ... 89
6 Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware ... 91
6.1 Neustart durchführen ... 91
6.2 Recovery-Prozedur ausführen ... 91
6.3 Flashen der Firmware ... 91
Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server ... 92
6.3.1 DHCP- und TFTP-Server unter Windows bzw. Linux installieren ... 94
Unter Windows: ... 94
Unter Linux ... 95
7 Glossar ... 96
Asymmetrische Verschlüsselung ... 96
DES / 3DES ... 96
AES ... 96
Client / Server ... 96
Datagramm ... 97
DynDNS-Anbieter ... 97
IP-Adresse ... 98
IPsec ... 99
NAT (Network Address Translation) ... 99
Port-Nummer ... 99
PPPoE ... 99
PPTP ... 100
X.509 Zertifikat ... 100
Protokoll, Übertragungsprotokoll ... 100
Service Provider ... 100
Spoofing, Antispoofing ... 100
Symmetrische Verschlüsselung ... 101
TCP/IP (Transmission Control Protocol/Internet Protocol) ... 101
VLAN ... 101
VPN (Virtuelles Privates Netzwerk) ... 101
8 Technische Daten ... 102

1 Einleitung

Der mGuard delta sichert IP-Datenverbindungen. Dazu vereinigt das Gerät folgende Funktionen:

- Switch
- VPN-Router (VPN - **V**irtuelles **P**rivates **N**etzwerk) für sichere Datenübertragung über öffentliche Netze (hardwarebasierte DES, 3DES und AES Verschlüsselung, IPsec Protokoll)
- Konfigurierbare Firewall für den Schutz vor unberechtigtem Zugriff. Der dynamische Paketfilter untersucht Datenpakete anhand der Ursprungs- und Zieladresse und blockiert unerwünschten Datenverkehr.
- Kaspersky-Virenschutz mit Unterstützung für die Protokolle HTTP, SMTP und POP3

Die Konfiguration des Gerätes erfolgt einfach mit einem Web-Browser.

Netzwerk-Features

- Stealth (Auto, Static, Multi), Router (Static, DHCP Client), PPPoE (für DSL) und PPTP (für DSL)
- VLAN
- DHCP Server/Relay auf den internen und externen Netzwerkschnittstellen
- DNS Cache auf den internen Netzwerkschnittstelle
- Administration über HTTPS und SSH

Firewall-Features

- Stateful Packet Inspection
- Anti-Spoofing
- IP Filter
- L2 Filter (nur im Stealth Mode)
- NAT mit FTP, IRC und PPTP Unterstützung (nur in den Router Modi)
- 1:1 NAT (nur in den Router Modi)
- Port Forwarding (nur in den Router Modi)
- Firewalldurchsatz maximal 99MBit/s

Anti-Virus-Features

- Kaspersky-Virenschutz
- Unterstützte Protokolle: HTTP, FTP, POP3 und SMTP (senden)

VPN-Features

- Protokoll: IPsec (Tunnel und Transport Mode)
- IPsec DES Verschlüsselung mit 56 Bit
- IPsec 3DES Verschlüsselung mit 168 Bit
- IPsec AES Verschlüsselung mit 128, 192 und 256 Bit
- Paket-Authentifizierung: MD5, SHA-1
- Internet Key Exchange (IKE) mit Main und Quick Mode
- Authentisierung: Pre-Shared Key (PSK), X.509v3 Zertifikate
- DynDNS
- NAT-T
- Dead Peer Detection (DPD)
- Hardware Verschlüsselung
- 250 VPN Tunnel
- VPN Durchsatz max. 35MBit/s bei 266MHz und 70MBit/s bei 533MHz

Weitere Features

- MAU Management
- Remote Logging
- Router/Firewall Redundanz
- IPsec/L2TP Server
- LLDP
- Administration using SNMP v1-v3 und Innominate Security Configuration Manager (ISCM)

Die folgende Tabelle gibt eine Übersicht über welche Eigenschaften die jeweili-

gen mGuard Modelle und Lizenzen verfügen:

		Lizenz				
		professional		enterprise FW	enterprise	enterprise XL
Model	smart	X	X		X	X
	pci		X		X	X
	delta		X		X	X
	industrial			X		X
	blade				X	X
Hardware	MHz	266	266	533	266	533
	RAM	64	64	64	64	64
	Flash	16	16	16	16	16
Eigenschaften	VPN Tunnel	2			10	250
	IPsec/L2TP Server				X	X
	MAU Management		X	X	X	X
	Remote Logging		X	X	X	X
	SNMP		X	X	X	X
	LLDP		X	X	X	X
	Redundanz			X		X

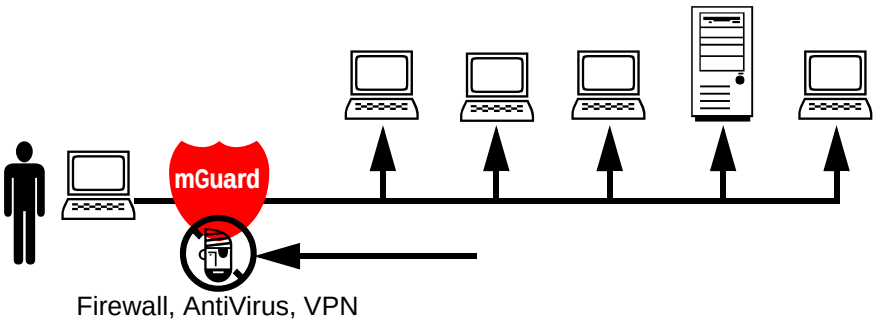
Support

Bei Problemen mit Ihrem mGuard wenden Sie sich bitte an Ihren Händler. Zusätzliche Informationen zum Gerät, sowie Release Notes und Software-Updates finden Sie unter folgender Internet-Adresse: http://www.innominate.de/

2 Typische Anwendungsszenarien

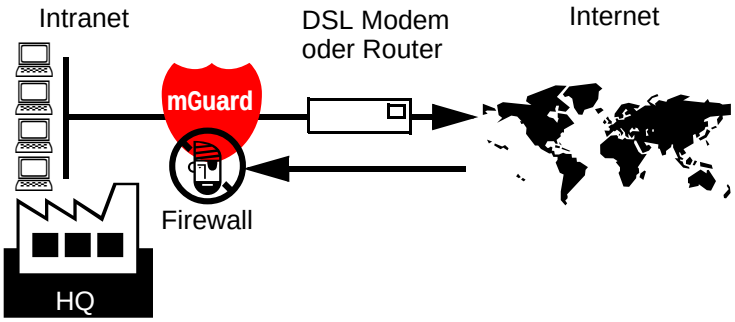
Nachfolgend werden häufige und typische Anwendungsszenarien skizziert.

Stealthmodus



Im *Stealth* Modus (Werkseinstellung) kann der mGuard zwischen einen einzelnen Rechner und das übrige Netzwerk gesetzt werden.
Die Einstellungen für Firewall, AntiVirus und VPN können mit einem Webbrowser unter der URL https://1.1.1.1/ vorgenommen werden.
Auf dem Rechner selbst müssen keine Konfigurationsänderungen durchgeführt werden.

Netzwerkrouter

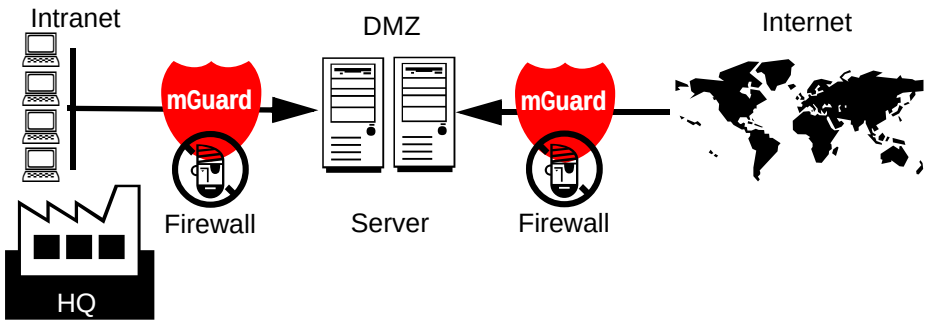


Der mGuard kann für mehrere Rechner als Netzwerkrouter die Internetanbindung bereitstellen und das Firmennetz dabei mit seiner Firewall schützen.
Dazu kann einer der folgenden Netzwerk-Modi des mGuard genutzt werden:

- *Router*, wenn der Internet-Anschluss z.B. über einen DSL-Router oder eine Standleitung erfolgt.
- *PPPoE*, wenn der Internet-Anschluss z.B. per DSL-Modem erfolgt und das PPPoE-Protokoll verwendet wird (z.B. in Deutschland).
- *PPTP*, wenn der Internet-Anschluss z. B. per DSL-Modem erfolgt und das PPTP-Protokoll verwendet wird (z. B. in Österreich).

Bei Rechnern im Intranet muss der mGuard als Defaultgateway festgelegt sein.

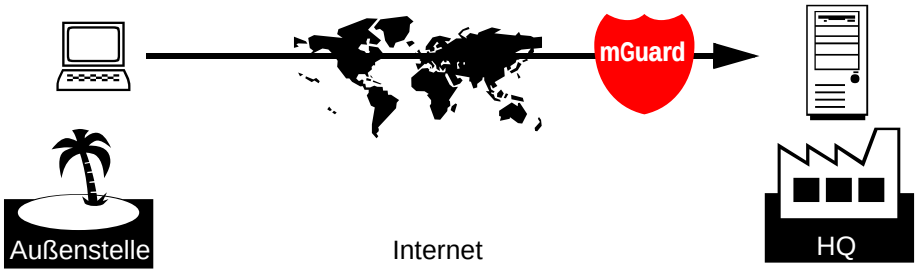
DMZ



Eine DMZ (Demilitarized Zone, deutsch: entmilitarisierte Zone) ist ein geschütztes Netzwerk, das zwischen zwei anderen Netzen liegt. Z.B. kann sich die Webpräsenz einer Firma so in der DMZ befinden, dass nur aus dem Intranet heraus mittels FTP neue Seiten auf den Server kopieret werden können, der lesende Zugriff per HTTP auf die Seiten jedoch auch aus dem Internet heraus möglich ist.

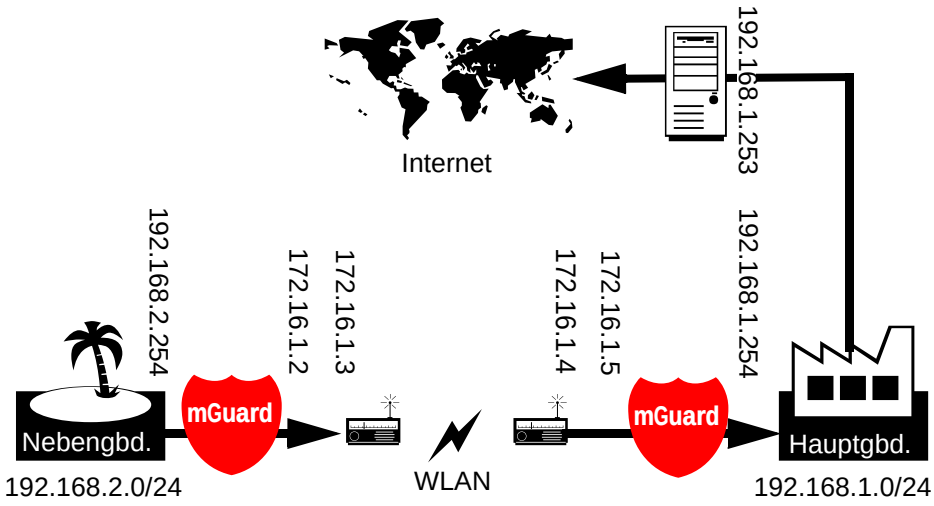
Die IP Adressen innerhalb der DMZ können öffentlich sein, oder aber privat, wobei der mit dem Internet verbundene mGuard die Verbindungen mittels Port-forwarding an die privaten Adressen innerhalb der DMZ weiterleitet.

VPN Gateway



Mitarbeitern einer Firma soll ein verschlüsselter Zugang zum Firmennetz von zu Hause oder von unterwegs aus zur Verfügung gestellt werden. Der mGuard übernimmt dabei die Rolle des VPN Gateways.
Auf den externen Rechnern muß dazu eine IPsec fähige VPN-Client Software installiert werden bzw. das Betriebssystem muß diese Funktionalität bereits unterstützen, wie z.B. Windows 2000/XP.

WLAN über VPN



Zwei Gebäude einer Firma sollen über eine mit IPsec geschützte WLAN Strecke miteinanderverbunden werden. Vom Nebengebäude soll zudem der Internetzugang des Hauptgebäudes mitgenutzt werden können.

In diesem Beispiel wurden die mGuards in den *Router*modus geschaltet und für das WLAN ein eigenes Netz mit 172.16.1.x Adressen eingerichtet.
Da vom Nebengebäude aus das Internet über das VPN erreichbar sein soll, wird hier eine Default Route über das VPN eingerichtet:

Verbindungstyp	Tunnel (Netz <-> Netz)
Adresse des lokalen Netzes	192.168.2.0/24
Adresse des gegenüberliegenden Netzes	0.0.0.0/0

Im Hauptgebäude wird das entsprechende Gegenstück der Verbindung konfiguriert:

Verbindungstyp	Tunnel (Netz <-> Netz)

Die dazugehörige Netzmaske	0.0.0.0
Adresse des gegenüberliegenden Netzes	192.168.2.0/24

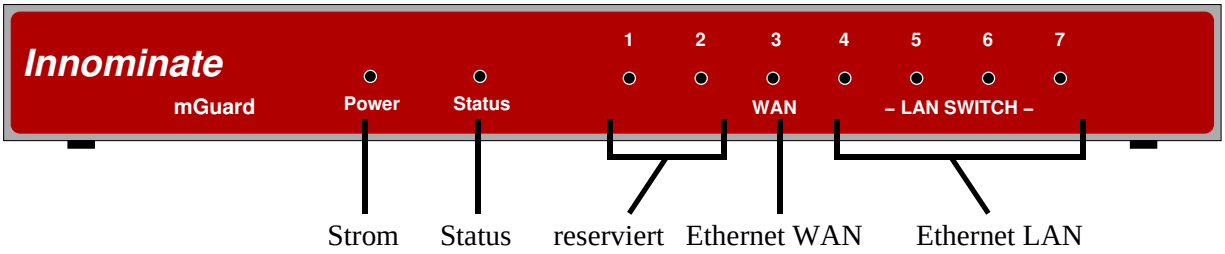
Die Default Route eines mGuards führt normalerweise immer über das externe Interface. In diesem Fall führt der Weg ins Internet und somit auch die Default Route, über die IP 192.168.1.253. Dazu muß beim mGuard im Hauptgebäude unter „Netzwerk > Basis“ eine interne Default Route definiert werden

Zusätzliche interne Routen	Netzwerk	Gateway
	0.0.0.0/0	192.168.1.253

und eine externe Route auf die IPs 172.168.1.2 und 172.168.1.3 eingerichtet werden

Zusätzliche externe Routen	Netzwerk	Gateway
	172.16.1.2/1	172.16.1.4

3 Bedienelemente und Anzeigen



LEDs	State	Meaning
Power	ein	Die Stromversorgung ist aktiv.
Status	ein	Der mGuard startet.
	Herzschlag (aufleuchten, aufleuchten, pause, ...)	The mGuard ist bereit.
1,2	-	Reserviert.
3 (WAN)	ein	Link vorhanden.
	blinkend	Datentransfer.
4-7 (LAN)	ein	Link vorhanden.
	blinkend	Datentransfer.

4 Inbetriebnahme

Sicherheits-hinweise

Der Innominate mGuard ist für den Betrieb bei Schutzkleinspannung vorgesehen. Schließen Sie die Netzwerkinterfaces des mGuard nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen. Der mGuard darf nicht an Fernmeldeanschlüssen betrieben werden.

Warnung! Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Massnahmen durchzuführen.

Allgemeine Hinweise zur Benutzung

- Umgebungsbedingungen:
  0 bis +° Celsius,
  max. Luftfeuchtigkeit %, nicht kondensierend
- Anschlusskabel nicht knicken. Den Netzwerkstecker nur zum Verbinden mit einem Netzwerk benutzen.

Schritte zur Inbetriebnahme

Um das Gerät in Betrieb zu nehmen, führen Sie folgende Schritte in der angegebenen Reihenfolge aus:

Schritt	Ziel	Seite
1	Lieferumfang prüfen, Release Notes lesen	„Lieferumfang” auf Seite 10
	Das Gerät konfigurieren, soweit erforderlich. Gehen Sie dazu die einzelnen Menüoptionen durch, die Ihnen der mGuard delta mit seiner Konfigurationsoberfläche bietet. Lesen Sie deren Erläuterungen in diesem Handbuch, um zu entscheiden, welche Optionen mit welcher Einstellung für Ihre Betriebsumgebung erforderlich oder gewünscht wird.	„Lokale Konfiguration: Bei Inbetriebnahme” auf Seite 11

4.1 Lieferumfang

Prüfen Sie vor Inbetriebnahme die Lieferung auf Vollständigkeit:

Zum Lieferumfang gehören

- Handbuch im Portable Document Format (PDF) auf CD
- Quick Installation Guide

5 Konfiguration

Voraussetzungen

- Der mGuard muss an seine Stromversorgung angeschlossen sein.
- Bei lokaler Konfiguration: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  – am LAN Switch (Ethernetbuchse 4 bis 7) des mGuard angeschlossen sein,
  – oder er muss über das lokale Netzerk mit ihm verbunden sein.
- Bei Fernkonfiguration: Der mGuard delta muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Der mGuard muss angeschlossen sein, d.h. die erforderlichen Verbindungen müssen funktionieren.

5.1 Lokale Konfiguration: Bei Inbetriebnahme

Der mGuard delta wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird (z. B. MS Internet-Explorer ab Version 5.0 oder Netscape Communicator ab Version 4.0)

⌧ Der Web-Browser muss SSL (d. h. https) unterstützen.

Der mGuard ist gemäß Werkseinstellung unter folgender Adressen erreichbar:

Werkseinstellung:	
Router-Modus (Auslieferungszustand)	https://192.168.1.1/

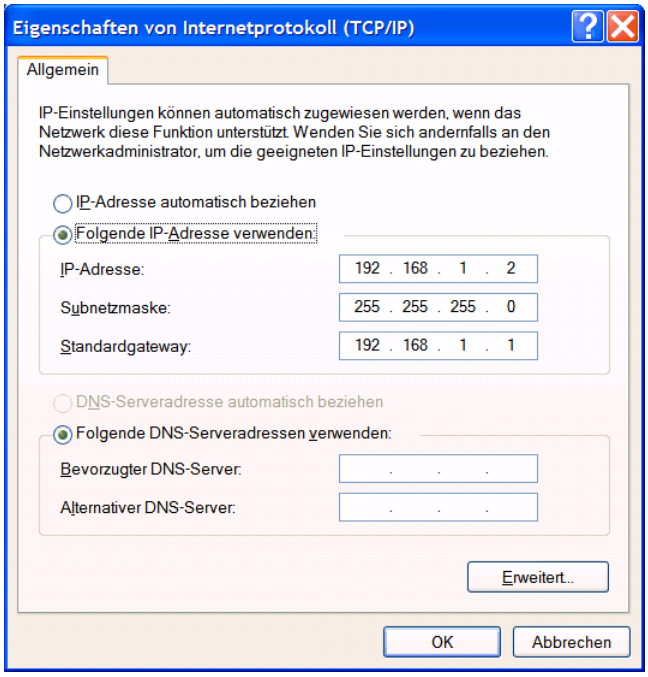
Erster Zugriff auf den mGuard

Bei Auslieferung oder nach Zurücksetzen auf die Werkseinstellung oder Flashen des mGuards ist der mGuard über die LAN Schnittstellen 4 bis 7 unter der IP 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar. Für einen Zugriff auf die Konfigurationsoberfläche kann es daher nötig sein, die Konfigurations Ihres Computer anzupassen.

Unter Windows XP klicken Sie dazu **Start, Systemsteuerung, Netzwerkverbindungen**:

- Das Symbol des LAN-Adapters mit der rechten Maustaste klikken und
- im Kontextmenü **Eigenschaften** klicken.
- Im Dialogfeld *Eigenschaften von LAN-Verbindung lokales Netz* auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren und dann
- die Schaltfläche **Eigenschaften** klicken, so dass folgendes Dialogfeld ange-

zeigt wird:


Eigenschaften von Internetprotokoll (TCP/IP)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 2
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway: 192 . 168 . 1 . 1
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Erweitert...
OK
Abbrechen

Aktivieren Sie zunächst **Folgende IP-Adressen verwenden** und geben dann zum Beispiel folgende Adressen ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standardgateway:	192.168.1.2

⌦ Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.2 Lokale Konfigurationsverbindung herstellen

Web-basierte Administrator-oberfläche

Der mGuard wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird (z. B. Firefox, MS Internet-Explorer oder Safari).

⌦ **Der Web-Browser muss SSL (d. h. https) unterstützen.**

Je nach dem, in welchem Netzwerk-Modus (= Betriebsart) der mGuard sich befindet, ist er gemäß Werkseinstellung unter einer der folgenden Adressen erreichbar:

Werkseinstellung:

Stealth-Modus (Auslieferungszustand):	https://1.1.1.1/
Router- / PPPoE- / PPPT-Modus:	https://192.168.1.1/

Gehen Sie wie folgt vor:

1. Starten Sie einen Web-Browser.
   (Z. B. Firefox, MS Internet-Explorer oder Safari; der Web-Browser muss SSL (d. h. https) unterstützen.)
2. Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum mGuard erschwert werden könnte.
   Im MS Internet Explorer nehmen Sie diese Einstellung wie folgt vor: Menü **Extras, Internetoptionen...**, Registerkarte *Verbindungen*:

Unter *DFÜ- und VPN-Einstellungen* muss **Keine Verbindung wählen** aktiviert sein.

3. In der Adresszeile des Web-Browsers geben Sie die Adresse des mGuard vollständig ein.

IP-Adresse des mGuard im *Stealth*-Modus: **https://1.1.1.1/**

Im **Stealth**-Modus lautet diese immer

`https://1.1.1.1/`

wenn nicht im *Stealth*-Modus: **https://192.168.1.1/**

und in den Betriebsarten **Router (= Werkseinstellung)**, **PPPoE** oder **PPTP** lautet diese immer

`https://192.168.1.1/`

Folge:
Sie gelangen zur Administrator-Website des mGuard. Der auf der nächsten Seite abgebildete Sicherheitshinweis erscheint.

⌧ Falls Sie die konfigurierte Adresse vergessen haben:

Falls die Adresse des mGuard im *Router- PPPoE-* oder *PPTP*-Modus auf einen anderen Wert gesetzt ist und Sie kennen die aktuelle Adresse nicht, dann müssen Sie den mGuard mit Hilfe der **Recovery**-Taste in den Stealth-Modus stellen und damit auf folgende Adresse: https://1.1.1.1/ (siehe „Recovery-Prozedur ausführen“ auf Seite 91).

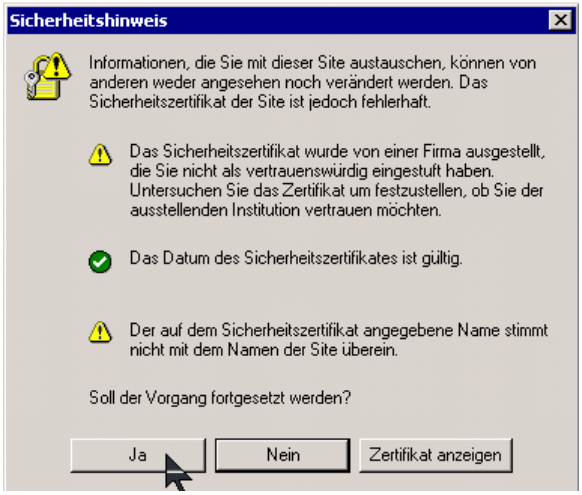
⌧ Falls die Administrator-Website nicht angezeigt wird...

Sollte auch nach wiederholtem Versuch der Web-Browser melden, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Prüfen Sie, ob der Standardgateway des angeschlossenen Konfigurations-Rechners initialisiert ist. Siehe „Lokale Konfiguration: Bei Inbetriebnahme“ auf Seite 11
- Eine bestehende Firewall gegebenenfalls deaktivieren.
- Achten Sie darauf, dass der Browser keinen Proxy Server verwendet.
  Im MS Internet Explorer (Version 6.0) nehmen Sie diese Einstellung wie folgt vor: Menü **Extras, Internetoptionen...**, Registerkarte *Verbindungen*: Unter *LAN-Einstellungen* auf die Schaltfläche **Einstellungen...** klicken, im Dialogfeld *Einstellungen für lokales Netzwerk (LAN)* dafür sorgen, dass unter Proxyserver der Eintrag **Proxyserver für LAN verwenden** nicht aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Unter Windows Menü **Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen** bzw. **Netzwerk- und DFÜ-Verbindungen** das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü **Deaktivieren** wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint dieser Sicherheitshinweis (MS Internet-Explorer):


Sicherheitshinweis
Informationen, die Sie mit dieser Site austauschen, können von anderen weder angesehen noch verändert werden. Das Sicherheitszertifikat der Site ist jedoch fehlerhaft.
Das Sicherheitszertifikat wurde von einer Firma ausgestellt, die Sie nicht als vertrauenswürdig eingestuft haben. Untersuchen Sie das Zertifikat um festzustellen, ob Sie der ausstellenden Institution vertrauen möchten.
Das Datum des Sicherheitszertifikates ist gültig.
Der auf dem Sicherheitszertifikat angegebene Name stimmt nicht mit dem Namen der Site überein.
Soll der Vorgang fortgesetzt werden?
Ja
Nein
Zertifikat anzeigen

Erläuterung:
Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

Quittieren Sie den entsprechenden Sicherheitshinweis mit **Ja**.

Folge:
Nach Abfrage des Benutzernamens (Login) und Passwortes wird die Administrator-Website des mGuard angezeigt.
Werksseitig ist voreingestellt:

Login: `admin`
Passwort: `mGuard`

⌦ Groß- und Kleinschreibung beachten!
Zur Konfiguration gehen Sie wie folgt vor:

Konfiguration durchführen

1. Über das Menü zur linken die Seite mit den gewünschten Einstellmöglichkeiten aufrufen - siehe ab Seite 16.
2. Auf der betreffenden Seite die gewünschten Einträge machen
3. Mit **OK** bestätigen, so dass die Einstellungen vom Gerät übernommen werden.
   Sie erhalten vom System eine (bestätigende) Rückmeldung.

Sollte bei erneuter Anzeige einer Seite diese nicht aktuell sein, weil der Browser sie aus dem Cache lädt, aktualisieren Sie die Anzeige der Seite. Dazu in der Browser-Symbolleiste das Symbol zum Aktualisieren klicken.

⌦ Je nach dem, wie Sie den mGuard konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

5.3 Fernkonfiguration

Voraussetzung

Der mGuard muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

⌦ Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Um die Möglichkeit zur Fernkonfiguration einzuschalten, siehe Abschnitt „Zugang → HTTPS“ auf Seite 72.

Fernkonfiguration durchführen

Um von einem entfernten Rechner aus den mGuard zu konfigurieren, stellen Sie von dort die Verbindung zum lokalen mGuard her.

Gehen Sie wie folgt vor:

1. Starten Sie dazu auf dem entfernten Rechner den Web-Browser (z. B.Firefox, MS Internet-Explorer oder Safari; der Web-Browser muss SSL (d. h. https) unterstützen.)
2. Als Adresse geben Sie an: Die IP-Adresse, unter der die Gegenstelle über das Internet bzw. WAN erreichbar ist, zusätzlich die Port-Nummer.

   Beispiel:
   Ist dieser mGuard über die Adresse 123.456.789.21 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: 123.456.789.21
   Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B.: 123.456.789.21:442

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern - siehe „Zugang → Passworte“ auf Seite 71.

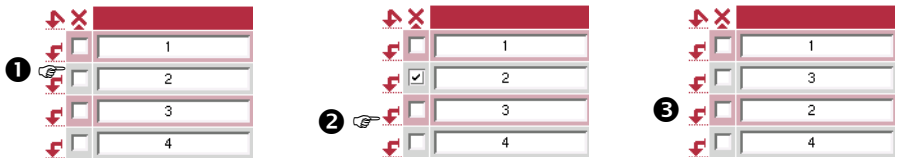
5.4 Arbeiten mit Tabellen

Einfügen von Zeilen

1. Klicken Sie auf den Pfeil, unter dem Sie eine neue Zeile einfügen wollen:

2. Die neue Zeile ist eingefügt.

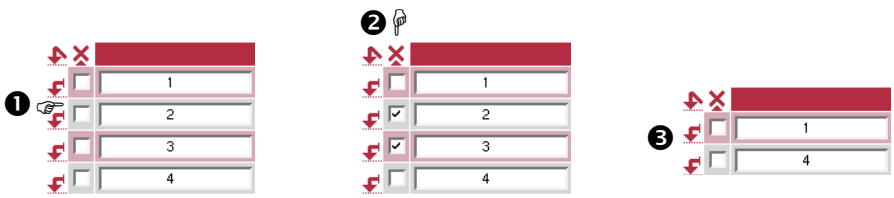
Verschieben von Zeilen



1. Markieren Sie eine oder mehrere Zeilen, die Sie verschieben wollen.
2. Klicken Sie auf den Pfeil, unter den Sie die markierten Zeilen verschieben wollen:

3. Die Zeilen sind verschoben.

Löschen von Zeilen



1. Markieren Sie die Zeilen, die Sie löschen wollen.
2. Klicken Sie auf das Zeichen zum Löschen:

3. Die Zeilen sind gelöscht.

5.5 Startseite

Auf der Startseite können Sie verschiedene Informationen eintragen, die Ihnen und anderen bei der Administration des mGuards helfen können:

Hostname
Der Hostname dieses mGuards.

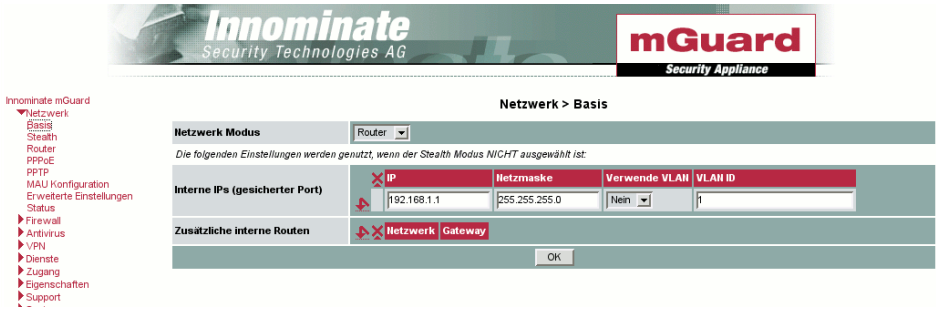
Kontakt
Name der Person, die diesen mGuard verwaltet und wie man sie erreichen kann.

Standort
Standort, an dem sich dieser mGuard befindet.

⌦ Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administratorpasswort zu ändern - siehe „Zugang → Passworte“ auf Seite 71. Solange dies noch nicht geschehen ist, erhalten Sie auf der Startseite einen Hinweis darauf.

5.6 Menü Netzwerk

Netzwerk → Basis



Netzwerk Modus
Der mGuard muss auf den Netzwerk-Modus (= Betriebsart) gestellt werden, der seiner lokalen Rechner- bzw. Netzwerk-Anbindung entspricht. Siehe „Typische Anwendungsszenarien“ auf Seite 6.

⌦ Beim Wechsel des Netzwerk-Modus in oder aus dem *Stealth*-Modus bootet das Gerät automatisch neu.

⌦ Wenn Sie die Adresse des mGuard ändern (z. B. durch Wechsel des Netzwerk-Modus von *Stealth* auf *Router*), dann ist das Gerät nur noch unter der neuen Adresse zu erreichen. Erfolgte die Änderung über das lokale Interface, so erhalten Sie eine Rückmeldung über die neue Adresse bevor die Änderung aktiv wird. Bei Änderungen vom externen Interface aus erhalten Sie keine Rückmeldungen.

- Wenn Sie den Modus auf *Router* oder *PPPoE* oder *PPTP* stellen und dann die interne IP-Adresse und/oder die lokale Netzmaske ändern, achten Sie unbedingt darauf, dass Sie korrekte Werte angeben. Sonst ist der mGuard nicht mehr erreichbar.

Transparenter mGuard

Stealth

Der *Stealth*-Modus wird ausschließlich zur lokalen Anbindung eines einzelnen Computers als Client verwendet.

In dieser Betriebsart kann das Gerät einfach in eine bestehende Netzwerkanbindung des betreffenden Rechners integriert werden. Der mGuard analysiert den laufenden Netzwerkverkehr und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig und arbeitet transparent, d. h. ohne dass der Client umkonfiguriert werden muss.

Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN zur Verfügung.

Von extern gelieferte DHCP-Daten werden an den angeschlossenen Client durchgelassen.

- Eine auf dem Client installierte Firewall muß ICMP Echo Requests (Ping) zulassen, wenn der mGuard Dienste die VPN, DNS, NTP, etc. nutzen soll.
- Die Einträge unter *Interne IPs* und *Zusätzliche interne Routen* werden im *Stealth* Modus ignoriert. Als interne IP wird stattdessen die 1.1.1.1 verwendet, die vom Client erreichbar ist, wenn auch das auf dem Client konfigurierte Defaultgateway erreichbar ist.

mGuard als Router

Der mGuard arbeitet auch im PPPoE- oder PPTP-Modus als Router.

Router (Werkseinstellung)

Befindet sich der mGuard nicht im *Stealth*-Modus, arbeitet er als Gateway zwischen verschiedenen Teilnetzen und hat dabei eine externe und eine interne IP-Adresse.

Der mGuard ist über seine externe Schnittstelle per Ethernet-Standleitung ans Internet angeschlossen oder über weitere Router ans LAN.

Ein Netzwerk oder ein Einzelrechner ist über sein internes Interface angeschlossen. Wie auch in den anderen Modi stehen die Sicherheitsfunktionen Firewall und VPN zur Verfügung.

- Wird der mGuard im *Router*-Modus betrieben, muss beim lokal angeschlossenen Client-Rechnern der mGuard als Defaultgateway festgelegt sein. D. h. die Adresse des Defaultgateway ist auf die interne IP des mGuard zu setzen. Siehe „IP-Konfiguration bei Windows-Clients“ auf Seite 66.
- Wird der mGuard im *Router*-Modus betrieben und stellt die Verbindung zum Internet her, sollte NAT aktiviert werden, um aus dem lokalen Netz heraus Zugriff auf das Internet zu erhalten - siehe „Firewall → NAT“ auf Seite 29. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

PPPoE

Der *PPPoE*-Modus entspricht dem Router-Modus mit DHCP - mit einem Unterschied: Für den Anschluss ans externe Netzwerk (Internet, WAN) wird - wie in Deutschland - das PPPoE-Protokoll verwendet, das von vielen DSL-Modems (bei DSL-Internetzugang) verwendet wird. Die externe IP-Adresse, unter der der mGuard von einer entfernten Gegenstelle aus erreichbar ist, wird vom Provider festgelegt.

- Wird der mGuard im *PPPoE*-Modus betrieben, muss bei lokal angeschlossenen Client-Rechnern der mGuard als Defaultgateway festgelegt sein. D. h. die Adresse des Defaultgateway ist auf die interne IP des mGuard zu setzen. Siehe „IP-Konfiguration bei Windows-Clients“ auf Seite 66.
- Arbeitet der mGuard im *PPPoE*-Modus, muss NAT aktiviert werden, um Zu-

griff auf das Internet zu erhalten - siehe „Firewall → NAT“ auf Seite 29. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

PPTP

Ähnlich dem *PPPoE*-Modus. In Österreich zum Beispiel wird statt des PPPoE-Protokolls das PPTP-Protokoll zur DSL-Anbindung verwendet.
(PPTP ist das Protokoll, das ursprünglich von Microsoft für VPN-Verbindungen benutzt worden ist.)

⌧ Wird der mGuard im *PPTP*-Modus betrieben, muss bei lokal angeschlossenen Client-Rechnern der mGuard als Defaultgateway festgelegt sein. D. h. die Adresse des Defaultgateway ist auf die interne IP des mGuard zu setzen. Siehe „IP-Konfiguration bei Windows-Clients“ auf Seite 66.

⌧ Wird der mGuard im *PPTP*-Modus betrieben, sollte NAT aktiviert werden, um aus dem lokalen Netz heraus Zugriff auf das Internet zu erhalten - siehe „Firewall → NAT“ auf Seite 29. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.

Interne IPs (gesicherter Port)

Interne IP ist die IP-Adresse, unter der der mGuard von Geräten des lokal angeschlossenen lokalen Netzes erreichbar ist.

Im **Stealth**-Modus lautet diese immer:

IP-Adresse:	**1.1.1.1**

Im **Router**- / **PPPoE**- / **PPTP**-Modus ist werksseitig voreingestellt:

IP-Adresse:	**192.168.1.1**
Lokale Netzmaske:	**255.255.255.0**

Sie können weitere Adressen festlegen, unter der der mGuard von Geräten des lokal angeschlossenen Netzes angesprochen werden kann. Das ist zum Beispiel dann hilfreich, wenn das lokal angeschlossene Netz in Subnetze unterteilt wird. Dann können mehrere Geräte aus verschiedenen Subnetzen den mGuard unter unterschiedlichen Adressen erreichen.

IP

IP-Adresse, unter welcher der mGuard am internen Interface erreichbar sein soll.

Netzmaske

Die Netzmaske des am internen Interface angeschlossenen Netzes.

Verwende VLAN

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **ja** zu setzen.

VLAN ID

Eine VLAN ID zwischen 1 und 4095.

☞ Eine Erläuterung des Begriffes „VLAN“ findet sich auf Seite 101.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.
(Die erste IP-Adresse in der Liste kann nicht gelöscht werden.)

⌧ Weitere festgelegte interne IPs haben im *Stealth*-Modus keine Wirkung. Im Stealth-Modus lautet die IP-Adresse immer: 1.1.1.1

Zusätzliche interne Routen (Nicht im Stealth-Modus)

Sind am lokal angeschlossen Netz weitere Subnetze angeschlossen, können Sie zusätzliche Routen definieren.

Netzwerk

Das Netzwerk in CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

Gateway

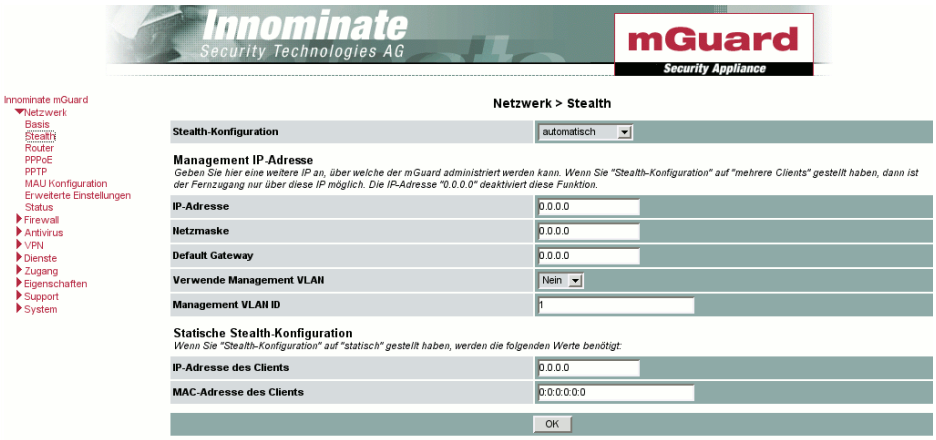
Das Gateway, über welches dieses Netzwerk erreicht werden kann.

☞ Siehe auch „Netzwerk-Beispielskizze“ auf Seite 89Mit einer internen Route nach 0.0.0.0/0 können Sie eine Default Route über das interne Interface definieren.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

⌦ Sind zusätzliche interne Routen festgelegt, haben diese im *Stealth*-Modus keine Wirkung.

Netzwerk → Stealth



Voraussetzung: Der mGuard ist auf den Netzwerk-Modus *Stealth* gestellt.

Stealth-Konfiguration

automatisch

(Standard) Der mGuard analysiert den Netzwerkverkehr, der über ihn läuft, und konfiguriert dementsprechend seine Netzwerkanbindung eigenständig und arbeitet transparent.

statisch

Wenn der mGuard keinen über ihn laufenden Netzwerkverkehr analysieren kann, z. B. weil zum lokal angeschlossenen Rechner nur Daten ein-, aber nicht ausgehen, dann muss die *Stealth-Konfiguration* auf **statisch** gesetzt werden.

mehrere Clients

Wie bei **automatisch**, es können jedoch mehr als nur einen Rechner bzw. mehrere IP-Adressen am internen Interface (gesicherter Port) des mGuard verwendet werden.

In diesem Modus ist die VPN Funktionalität des mGuard aus technischen Gründen deaktiviert.

Management IP-Adresse

Hier können Sie eine weitere IP-Adresse angeben, über welche der mGuard ad-

ministriert werden kann. Wenn

- unter *Stealth-Konfiguration* die Option **mehrere Clients** gewählt ist oder
- der Client ARP Anfragen nicht beantwortet oder
- kein Client vorhanden ist,

dann ist der Fernzugang über HTTPS, SNMP und SSH nur über diese Adresse möglich.

IP-Adresse

Die zusätzliche IP-Adresse, unter welcher der mGuard erreichbar sein soll. Die IP-Adresse „0.0.0.0“ deaktiviert die Management IP-Adresse.

Netzmaske

Die Netzmaske zu obiger IP-Adresse.

Default Gateway

Das Default Gateway des Netzes, in dem sich der mGuard befindet.

Verwende Management VLAN

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **ja** zu setzen.

Management VLAN ID

Eine VLAN ID zwischen 1 und 4095.

☞ Eine Erläuterung des Begriffes „VLAN“ findet sich auf Seite 101.

Statische Stealth-Konfiguration

IP-Adresse des Clients

Die IP-Adresse des Clients.

MAC-Adresse des Clients

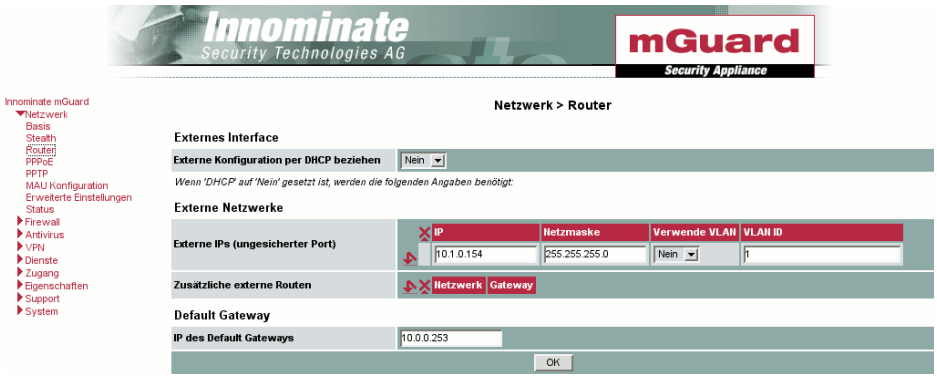
Das ist die physikalische Adresse der Netzwerkkarte des lokalen Rechners, an dem der mGuard angeschlossen ist.

☒ Die MAC-Adresse ermitteln Sie wie folgt:

Auf der DOS-Ebene (Menü **Start, Alle Programme, Zubehör, Eingabeaufforderung**) folgenden Befehl eingeben:

```
ipconfig /all
```

Netzwerk → Router



Voraussetzung: Der mGuard ist auf den Netzwerk-Modus *Router* gestellt.

Externes Interface

Externe Konfiguration per DHCP beziehen: Ja / Nein

☞ Falls der mGuard die Konfigurationsdaten per DHCP (Dynamic Host Configuration Protocol) vom DHCP-Server bezieht, legen Sie **Ja** fest. Dann bleiben weiter Angaben auf dieser Seite wirkungslos.

☞ Falls der mGuard die Daten nicht per DHCP (Dynamic Host Configuration Protocol) vom DHCP-Server bezieht, legen Sie **Nein** fest und

machen Sie die folgenden weiteren Angaben:

Externe Netwerke

Externe IPs

Die Adressen, unter denen der mGuard von Geräten des externen Netzes (angeschlossenen an der Ethernet-Buchse des mGuard) aus erreichbar ist. Sie bilden die Schnittstelle zu anderen Teilen des LAN oder zum Internet. Findet hier der Übergang zum Internet statt, werden die IP-Adressen vom Internet Service Provider (ISP) vorgegeben.

IP/Netzmaske

IP und Netzmaske für das externe Interface (WAN).

Verwende VLAN

Wenn die IP-Adresse innerhalb eines VLANs liegen soll, ist diese Option auf **ja** zu setzen.

VLAN ID

Eine VLAN ID zwischen 1 und 4095.

☞ Eine Erläuterung des Begriffes „VLAN“ findet sich auf Seite 101.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.
(Die erste IP-Adresse in der Liste kann nicht gelöscht werden.)

Zusätzliche externe Routen

Zusätzlich zur Default Route (s. u.) können Sie weitere externe Routen festlegen.

Netzwerk / Gateway

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Siehe auch „Netzwerk-Beispielskizze“ auf Seite 89.

Default Gateway

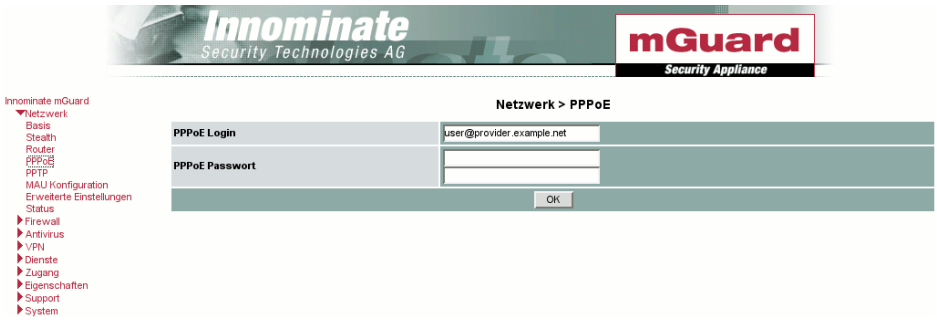
IP des Default Gateways

Wird vom Internet Service Provider (ISP) vorgegeben, wenn der mGuard den Übergang zum Internet herstellt. Wird der mGuard innerhalb des LANs eingesetzt, wird die Route vom Netzwerk-Administrator vorgegeben.

⌧ Diese Einstellung wird ignoriert, wenn eine lokale Default Route unter „Netzwerk → Basis“ definiert wurde.

⌧ Wenn das lokale Netz dem externen Router nicht bekannt ist, z. B. im Falle einer Konfiguration per DHCP, dann sollten Sie unter Firewall → NAT Ihr lokales Netz angeben, also 0.0.0.0/0 (siehe „Firewall → NAT“ auf Seite 29)

Netzwerk → PPPoE



Voraussetzung: Der mGuard ist auf den Netzwerk-Modus *PPPoE* gestellt. - sie-

he „PPPoE“ auf Seite 17.
Benutzername (Login) und Passwort werden vom Internet Service Provider (ISP) abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

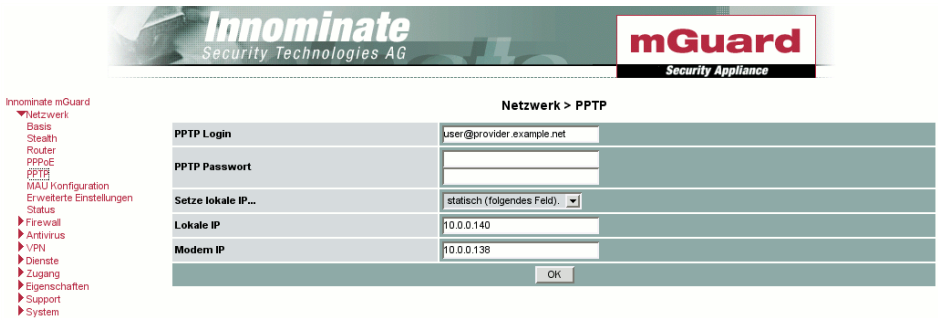
PPPoE Login

Benutzername (Login), den der Internet Service Provider (ISP) anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPPoE Passwort

Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

Netzwerk → PPTP



Voraussetzung: Der mGuard ist auf den Netzwerk-Modus *PPTP* gestellt. - siehe „PPTP“ auf Seite 18.
Benutzername (Login) und Passwort werden vom Internet Service Provider (ISP) abfragt, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPTP Login

Benutzername (Login), den der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

PPTP Passwort

Passwort, das der Internet Service Provider anzugeben fordert, wenn Sie eine Verbindung ins Internet herstellen wollen.

Setze lokale IP

Über DHCP

Werden die Adressdaten für den Zugang zum PPTP-Server vom Internet Service Provider per DHCP geliefert, wählen Sie **Über DHCP**.
Dann ist kein Eintrag unter **Lokale IP** zu machen.
Modem IP. Das ist die Adresse des PPTP-Servers des Internet Service Providers.

Statisch (folgendes Feld)

Werden die Adressdaten für den Zugang zum PPTP-Server nicht per DHCP vom Internet Service Provider geliefert, dann muss die IP-Adresse gegenüber dem PPTP-Server angegeben werden - als lokale IP-Adresse.

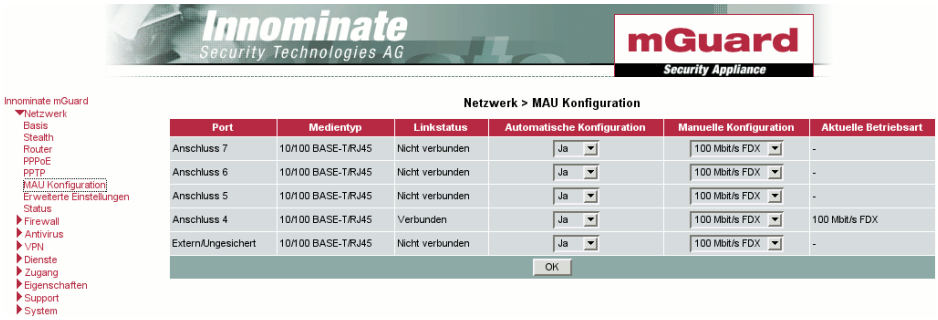
Lokale IP

IP-Adresse, unter der der mGuard vom PPTP-Server aus zu erreichen ist.

Modem IP

Das ist die Adresse des PPTP-Servers des Internet Service Providers.

Netzwerk → MAU Konfiguration



Konfiguration und Statusanzeige der Ethernetanschlüsse:

Port

Name des Ethernetanschlusses, auf welchen sich die Zeile bezieht.

Medientyp

Medientyp des Ethernetanschlusses.

Linkstatus

Up: Die Verbindung ist aufgebaut.

Down: Die Verbindung ist nicht aufgebaut.

Automatische Konfiguration

Ja: Versuche die benötigte Betriebsart eigenständig zu ermitteln.

Nein: Verwende die vorgegebene Betriebsart aus der Spalte „Manuelle Konfiguration“.

⌧ Beide Netzwerkschnittstellen des mGuard sind zur Verbindung mit einem Rechner konfiguriert. Beim Anschluß an einen Hub ist folgendes zu beachten: Bei deaktivierter *Automatischer Konfiguration* wird auch die Auto-MDIX Funktion deaktiviert, d.h. der Port des mGuard muß entweder an den Uplink-Port des Hub oder mittels eines Cross-Link-Kabels mit dem Hub verbunden werden.

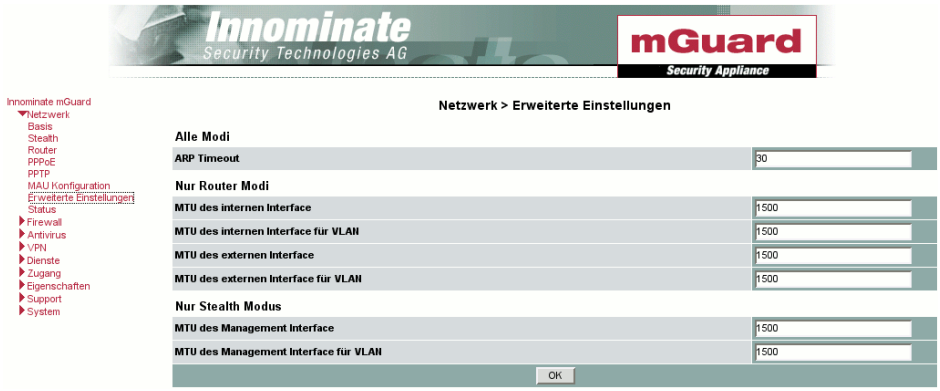
Manuelle Konfiguration

Die gewünschte Betriebsart, wenn *Automatische Konfiguration* auf *Nein* gestellt ist.

Aktuelle Betriebsart

Die aktuelle Betriebsart des Netzwerkanschlusses.

Netzwerk → Erweiterte Einstellungen



Alle Modi

ARP Timeout

Lebensdauer der Einträge in der ARP-Tabelle.

Nur Router Modi

MTU des ... Interface

Die Maximum Transfer Unit (MTU) beschreibt die maximale IP-Paketlänge, die genutzt werden darf.

Nur Stealth Modus

MTU des Management Interface

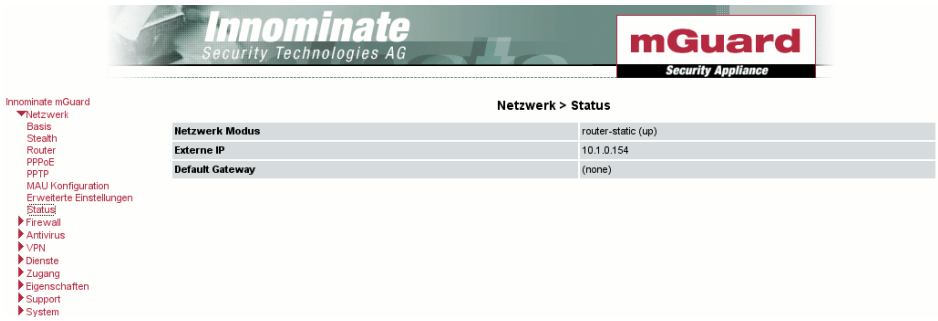
Die Maximum Transfer Unit (MTU) beschreibt die maximale IP-Paketlänge, die genutzt werden darf.

MTU des Management Interfaces für VLAN

Da die VLAN Pakete 4 Byte länger als Pakete ohne VLAN sind, haben bestimmte Treiber Probleme mit der Verarbeitung der größeren Pakete. Eine Reduzierung der MTU auf 1496 kann dieses Problem beseitigen.

Netzwerk → Status

Nur Anzeige



Netzwerk Modus

Zeigt die aktuelle Betriebsart des mGuard: *Stealth*, *Router*, *PPPoE* oder *PPTP*. Siehe „Netzwerk → Basis“ auf Seite 16.

Externe IP

Die IP-Adresse des mGuard an seinem Anschluss für das externe Netz (WAN bzw. Internet).

Wird dem mGuard eine IP-Adresse dynamisch zugeteilt, können Sie hier die gerade gültige IP-Adresse nachschlagen.

Im *Stealth*-Modus übernimmt der mGuard die Adresse des lokal angeschlossenen Rechners als seine externe IP.

Default Gateway

Hier wird die IP-Adresse angezeigt, über die der mGuard versucht ihm unbekannte Netze zu erreichen.Im *Stealth*-Modus oder falls die in der Konfiguration angegebene IP nicht erreichbar ist steht hier „(none)“.

5.7 Menü Firewall

Der mGuard beinhaltet eine *Stateful Packet Inspection Firewall*. Die Verbindungsdaten einer aktiven Verbindung werden in einer Datenbank erfasst (connection tracking). Dadurch sind Regeln nur für eine Richtung zu definieren, Daten aus der anderen Richtung einer Verbindung, und nur diese, werden automatisch durchgelassen. Ein Nebeneffekt ist, dass bestehende Verbindungen bei einer Umkonfiguration nicht abgebrochen werden, selbst wenn eine entsprechende neue Verbindung nicht mehr aufgebaut werden dürfte.

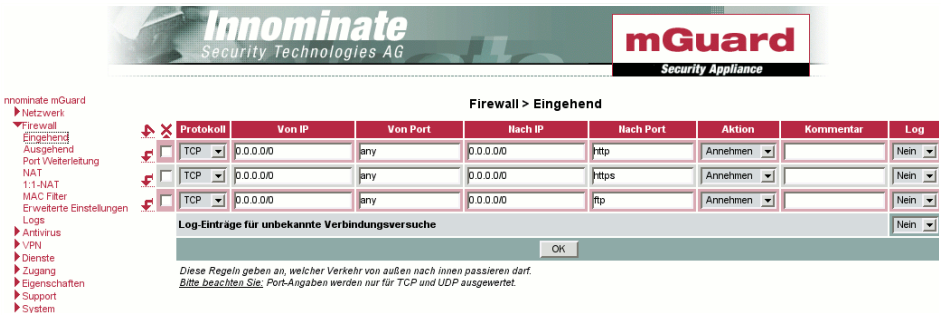
Werkseitige Voreinstellung der Firewall:

- Alle eingehenden Verbindungen werden abgewiesen (außer VPN).
- Die Datenpakete aller ausgehenden Verbindungen werden durchgelassen.

⌦ VPN-Verbindungen unterliegen nicht den unter diesem Menüpunkt festgelegten Firewall-Regeln. Firewall-Regeln für jede einzelne VPN-Verbindung können Sie unter Menü **VPN → Verbindungen** festlegen.

⌦ Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

Firewall → Eingehend



Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenverbindungen, die von extern initiiert wurden.
Ist keine Regel gesetzt, werden alle eingehenden Verbindungen (außer VPN) verworfen (= Werkseinstellung).

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

⌦ Durch die Aktivierung der Antivirusfunktion (siehe „Menü Antivirus“ auf Seite 34) werden implizit Firewallregeln für die Protokolle HTTP, SMTP und POP3 eingerichtet, die **nicht** in der Liste der Firewall-Regeln erscheinen.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

IP-Adresse

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.
Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.
Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)
Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

⌦ Im Stealth-Modus entspricht **Abweisen** aus der Aktion **Verwerfen**.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

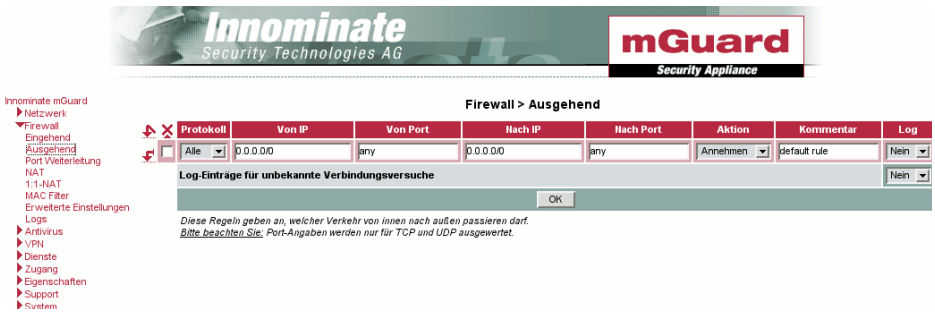
☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

Firewall → Ausgehend



Listet die eingerichteten Firewall-Regeln auf. Sie gelten für ausgehende Datenverbindungen, die von intern initiiert wurden, um mit einer entfernten Gegenstelle zu kommunizieren.
Per Werkseinstellung ist eine Regel gesetzt, die alle ausgehenden Verbindungen zulässt.
Ist keine Regel gesetzt, sind alle ausgehenden Verbindungen verboten (außer VPN).

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

IP-Adresse

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben, z. B. 110 für pop3 oder pop3 für 110.

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie *Verwerfen* (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

⌦ Im Stealth-Modus entspricht **Abweisen** aus der Aktion **Verwerfen**.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

Firewall → Port Weiterleitung

Listet die festgelegten Regeln zur Port-Weiterleitung auf.

Bei Port-Weiterleitung geschieht Folgendes: Der Header eingehender Datenpakete aus dem externen Netz, die an die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuard sowie an einen bestimmten Port des mGuard gerichtet sind, werden so umgeschrieben, dass sie ins interne Netz an einen bestimmten Rechner und zu einem bestimmten Port dieses Rechners weitergeleitet werden. D. h. die IP-Adresse und Port-Nummer im Header eingehender Datenpakete werden geändert.

Dieses Verfahren wird auch Destination-NAT genannt.

⌦ Die hier eingestellten Regeln haben Vorrang gegenüber den Einstellungen unter **Firewall → Eingehend**.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Protokoll

Geben Sie hier das Protokoll an, auf den sich die Regel beziehen soll.

Von IP

Absenderadresse, für die Weiterleitungen durchgeführt werden sollen.

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

Von Port

Absenderport, für den Weiterleitungen durchgeführt werden sollen.

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben, z. B. 110 für pop3 oder pop3 für 110.

Geben Sie hier das Protokoll an, auf den sich die Regel beziehen soll.

Eintreffend auf IP

Geben Sie hier die externe IP-Adresse (oder eine der externen IP-Adressen) des mGuard an.

ODER

Falls ein dynamischer Wechsel der externen IP-Adresse des mGUard erfolgt, so dass diese nicht angebbar ist, verwenden Sie folgende Variable: **%extern.**

⌧ Die Angabe von **%extern** bezieht sich bei der Verwendung von mehreren statischen IP-Adressen für das externe Interface immer auf die erste IP-Adresse der Liste.

Eintreffend auf Port

Original-Ziel-Port, der in eingehenden Datenpaketen angegeben ist.

Weiterleiten an IP

Interne IP-Adresse, an die die Datenpakete weitergeleitet werden sollen und auf die die Original-Zieladressen umgeschrieben werden.

Weiterleiten an Port

Port, an den die Datenpakete weitergeleitet werden sollen und auf den die Original-Port-Angaben umgeschrieben werden.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Bei den Angaben haben Sie folgende Möglichkeiten:

Port

Sie können nur einzelne Ports angeben, entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen: (z. B. 110 für pop3 oder pop3 für 110).

Log

Für jede einzelne Port-Weiterleitungs-Regel können Sie festlegen, ob bei Greifen der Regel

☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Firewall → NAT

Listet die festgelegten Regeln für NAT (**N**etwork **A**ddress **T**ranslation) auf.

Das Gerät kann bei ausgehenden Datenpaketen die angegebenen Absender-IP-Adressen aus seinem internen Netzwerk auf seine eigene externe Adresse umschreiben, eine Technik, die als NAT (Network Address Translation) bezeichnet wird.

Diese Methode wird benutzt, wenn die internen Adressen extern nicht geroutet werden können oder sollen, z. B. weil ein privater Adressbereich wie 192.168.x.x oder die interne Netzstruktur verborgen werden soll.

Dieses Verfahren wird auch *IP-Masquerading* genannt.

- Arbeitet der mGuard im *PPPoE/PPTP*-Modus, muss NAT aktiviert werden, um Zugriff auf das Internet zu erhalten. Ist NAT nicht aktiviert, können nur VPN-Verbindungen genutzt werden.
- Bei der Verwendung von mehreren statischen IP-Adressen für das externe Interface wird immer die erste IP-Adresse der Liste für IP-Masquerading verwendet.

Werkseinstellung: Es findet kein NAT statt.

> ☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Bei den Angaben haben Sie folgende Möglichkeiten:

Von IP

0.0.0.0/0 bedeutet alle Adressen, d. h. alle internen IP-Adressen werden dem NAT-Verfahren unterzogen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

Firewall → 1:1 NAT

Listet die festgelegten Regeln für 1:1 NAT (**N**etwork **A**ddress **T**ranslation) auf. Dabei spiegelt der mGuard die Adressen des internen Netzes in das externe Netz.

Im folgenden Beispiel befindet sich der mGuard mit der internen Schnittstelle im Netz 192.168.0.0/24 und mit der externen im Netz 10.0.0.0/24. Durch das 1:1 NAT läßt sich der Rechner 192.168.0.8 im externen Netz unter der IP 10.0.0.8 erreichen.

192.168.0.0/24 **10.0.0.0/24**

Werkseinstellung: Es findet kein 1:1 NAT statt.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

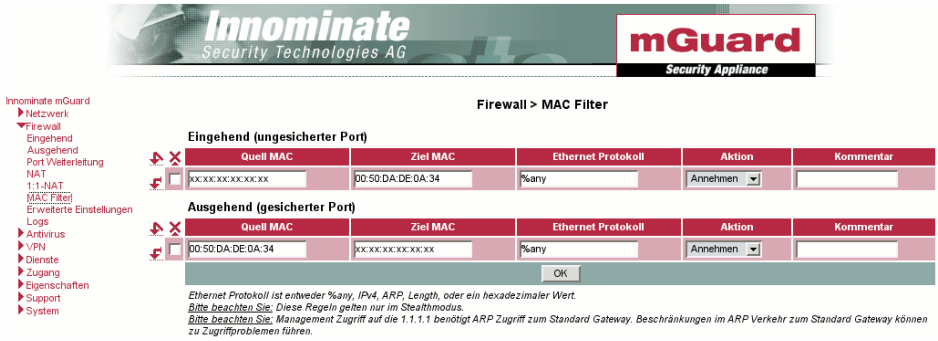
Bei den Angaben haben Sie folgende Möglichkeiten:

Lokales Netzwerk
Die Netzwerkadresse am lokalen Interface (LAN).

Externes Netzwerk
Die Netzwerkadresse am externen Interface (WAN).

Netzmaske
Die Netzmaske als Wert zwischen 1 und 32 für die lokale und externe Netzwerkadresse (siehe auch „CIDR (Classless InterDomain Routing)“ auf Seite 89).

Firewall → MAC Filter



Im Stealth Modus kann neben der IP Firewall (Layer 3/4), die den Datenverkehr z.B. nach ICMP Nachrichten oder TCP/UDP Verbindungen filtert, mit dem MAC Filter (Layer 2) nach MAC Adressen und Ethernet Protokollen gefiltert werden.
Im Gegensatz zur IP Firewall ist der MAC Filter stateless. Das heißt, werden Regeln eingeführt, müssen gegebenenfalls Regeln für die Gegenrichtung erstellt werden.

Ist keine Regel gesetzt, sind alle ARP und IP Packete erlaubt.

Quell MAC
Angabe der Quell MAC Adresse: xx:xx:xx:xx:xx:xx steht für alle MAC Adressen.

Ziel MAC
Angabe der Ziel MAC Adresse: xx:xx:xx:xx:xx:xx steht für alle MAC Adressen. Der Wert ff:ff:ff:ff:ff:ff ist die Broadcast MAC Adresse, an die z.B. alle ARP Anfragen geschickt werden.

Ethernet Protokoll

%any steht für alle Ethernet Protokolle. Weitere Protokolle können mit dem Namen oder in HEX angegeben werden, zum Beispiel:

- IPv4 oder 0800
- ARP oder 0806

Aktion

Annehmen bedeutet, die Datenpackete dürfen passieren

Verwerfen bedeutet, die Datenpackete werden verworfen

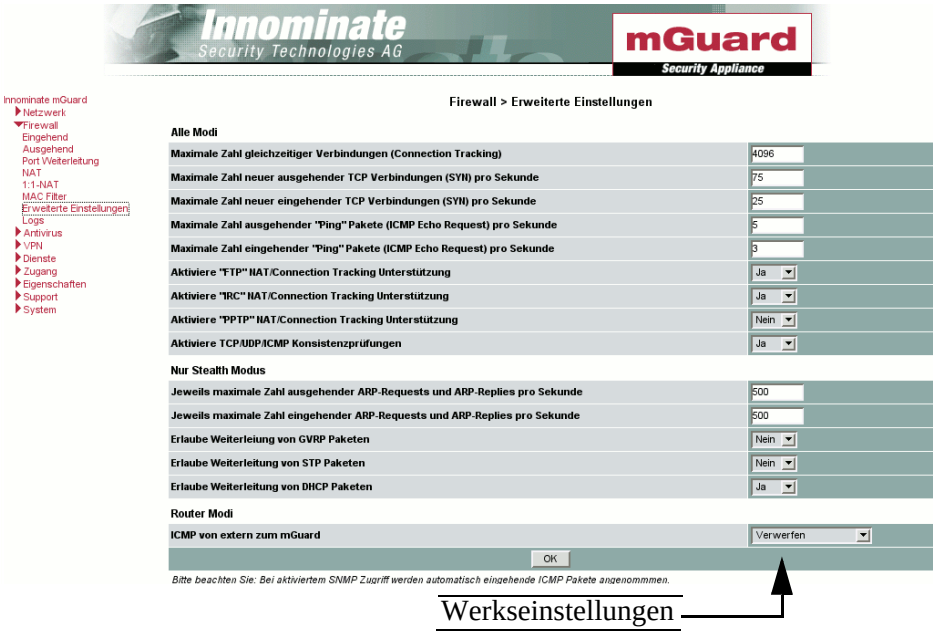
Kommentar

Ein frei wählbarer Kommentar für diese Regel.

☞ Der MAC Filter unterstützt keine Logging Funktionalität

☞ Die hier angegebenen Regeln haben Vorrang gegenüber den Firewall Regeln.

Firewall → Erweiterte Einstellungen


Innominate Security Technologies AG
mGuard Security Appliance
Innominate mGuard
Netzwerk
Firewall
Eingehend
Ausgehend
Port Weiterleitung
NAT
1:1-NAT
MAC Filter
Erweiterte Einstellungen
Logs
Antivirus
VPN
Dienste
Zugang
Eigenschaften
Support
System
Firewall > Erweiterte Einstellungen
Alle Modi
Maximale Zahl gleichzeitiger Verbindungen (Connection Tracking) 4096
Maximale Zahl neuer ausgehender TCP Verbindungen (SYN) pro Sekunde 75
Maximale Zahl neuer eingehender TCP Verbindungen (SYN) pro Sekunde 25
Maximale Zahl ausgehender "Ping" Pakete (ICMP Echo Request) pro Sekunde 5
Maximale Zahl eingehender "Ping" Pakete (ICMP Echo Request) pro Sekunde 3
Aktiviere "FTP" NAT/Connection Tracking Unterstützung Ja
Aktiviere "IRC" NAT/Connection Tracking Unterstützung Ja
Aktiviere "PPTP" NAT/Connection Tracking Unterstützung Nein
Aktiviere TCP/UDP/ICMP Konsistenzprüfungen Ja
Nur Stealth Modus
Jeweils maximale Zahl ausgehender ARP-Requests und ARP-Replies pro Sekunde 500
Jeweils maximale Zahl eingehender ARP-Requests und ARP-Replies pro Sekunde 500
Erlaube Weiterleiung von GVRP Paketen Nein
Erlaube Weiterleitung von STP Paketen Nein
Erlaube Weiterleitung von DHCP Paketen Ja
Router Modi
ICMP von extern zum mGuard Verwerfen
OK
Bitte beachten Sie: Bei aktiviertem SNMP Zugriff werden automatisch eingehende ICMP Pakete angenommen.
Werkseinstellungen

Die Einstellungen betreffen das grundlegende Verhalten der Firewall.

Alle Modi

Maximale Zahl ...

Diese 5 Einträge legen Obergrenzen fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

Aktiviere „FTP“ NAT/Connection Tracking Unterstützung

Wird beim FTP-Protokoll eine ausgehende Verbindung hergestellt, um Daten abzurufen, gibt es zwei Varianten der Datenübertragung: Beim „aktiven FTP“ stellt der angerufene Server im Gegenzug eine zusätzliche Verbindung zum Anrufer her, um auf dieser Verbindung die Daten zu übertragen. Beim „passiven FTP“ baut der Client diese zusätzliche Verbindung zum Server zur Datenübertragung auf. Damit die zusätzlichen Verbindungen von der Firewall durchgelassen werden, muss **Aktiviere „FTP“ NAT/Connection Tracking Unterstützung** auf **Ja** stehen (Standard).

Aktiviere „IRC“ NAT/Connection Tracking Unterstützung

Ähnlich wie bei FTP: Beim Chatten im Internet per IRC müssen nach aktivem Verbindungsaufbau auch eingehende Verbindungen zugelassen werden, soll das Chatten reibungslos funktionieren. Damit diese von der Firewall durchgelassen werden, muss **Aktiviere „IRC“ NAT/Connection Tracking Unterstützung** auf **Ja** stehen (Standard).

Aktiviere „PPTP“ NAT/Connection Tracking Unterstützung

Muss **Ja** gesetzt werden, wenn von lokalen Rechnern ohne Zuhilfenahme des mGuard VPN-Verbindungen mittels PPTP zu externen Rechner aufgebaut werden können sollen.

Werkseitig ist dieser Schalter auf **Nein** gesetzt.

Aktiviere TCP/UDP/ICMP Konsistenzprüfung

Wenn auf **Ja** gesetzt, führt der mGuard eine Reihe von Tests auf falsche Prüfsummen, Paketgrößen, usw. durch und verwirft diese Pakete.

Werkseitig ist dieser Schalter auf **Ja** gesetzt.

Nur Stealth Modus

Jeweils maximale Zahl ausgehender ARP-Requests ...

Jeweils maximale Zahl eingehender ARP-Requests ...

Diese beiden Einträge legen Maximalwerte für die zugelassenen ein- und ausgehenden ARP-Requests pro Sekunde fest. Diese sind so gewählt, dass sie bei normalem praktischen Einsatz nie erreicht werden. Bei Angriffen können sie dagegen leicht erreicht werden, so dass durch die Begrenzung ein zusätzlicher Schutz eingebaut ist. Sollten in Ihrer Betriebsumgebung besondere Anforderungen vorliegen, dann können Sie die Werte erhöhen.

Erlaube Weiterleitung von GVRP Paketen

Das GARP VLAN Registration Protocol (GVRP) wird von GVRP fähigen Switches verwendet um Konfigurationsinformationen miteinander auszutauschen.

Ist dieser Schalter auf **Ja** gesetzt, dann können GVRP Pakete den mGuard im Stealth Modus passieren.

Erlaube Weiterleitung von STP Paketen

Das Spawning-Tree Protocol (STP) (802.1d) wird von Bridges und Switches verwendet um Schleifen in der Verkabelung zu entdecken und zu berücksichtigen.

Ist dieser Schalter auf **Ja** gesetzt, dann können STP Pakete den mGuard im Stealth Modus passieren.

Erlaube Weiterleitung von DHCP Paketen

Erlaube dem Client über DHCP eine IP Adresse unabhängig von den ausgehenden Firewallregeln zu beziehen, da diese erst aktiv werden nachdem der mGuard die IP des Clients gelernt hat.

Die Voreinstellung für diesen Schalter ist **Ja**.

Router Modi

ICMP von extern zum mGuard

Mit dieser Option können Sie das Verhalten beim Empfang von ICMP-Nachrichten beeinflussen, die aus dem externen Netz an den mGuard gesendet werden. Sie haben folgende Möglichkeiten:

Verwerfen: Alle ICMP-Nachrichten zum mGuard werden verworfen.

Annehmen von Ping: Nur Ping-Nachrichten (ICMP Typ 8) zum mGuard werden akzeptiert.

Alle ICMPs annehmen: Alle Typen von ICMP Nachrichten zum mGuard werden akzeptiert.

Firewall → Logs

Nur Anzeige

Ist bei Festlegung von Firewall-Regeln das Protokollieren von Ereignissen festgelegt (Log = Ja), dann können Sie hier das Log aller protokollierten Ereignisse einsehen.

Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

5.8 Menü Antivirus

Der Antivirus-Funktion des Innominate mGuard schützt vor Viren, die über die Protokolle HTTP, POP3 und SMTP versendet werden.

Kaspersky Engine

Die übertragenen Datenblöcke einer E-Mail oder einer HTTP-Verbindung werden aus dem Datentransfer ausgefiltert, falls notwendig dekomprimiert, und durch den Kaspersky-Virenfilter überprüft.

Dazu wird für jedes unterstützte Protokoll eine Port-Redirection-Regel in die Firewall eingefügt, die eine interne Umleitung der Verbindung zu einem transparenten Proxy bewirkt.

Im Falle eines erkannten Virus wird je nach Protokoll entweder eine Fehlermeldung als E-Mail an den Nutzer gesendet, eine Protokollfehlermeldung generiert bzw. ein Eintrag im Antivirus-Log vorgenommen. Falls der Virenfilter keinen Virus findet, wird der Datenblock vom Proxy unverändert weitergesendet.

Details erfahren Sie in den folgenden Abschnitten zu den jeweiligen Protokollen.

Unterstützte Kompressionsformate

Der Virenfilter kann folgende Formate dekomprimieren:

- ZIP
- RAR
- Mail
- Embedded (RFC822 MIME Anhänge an E-Mails, MS OLE, inklusive gzipped embedded Skripte).
- GZIP
- Compress

Die Unterstützung weiterer Formate (Trap, UPX) ist in Vorbereitung.

Voraussetzungen zur Nutzung

Folgende Voraussetzungen müssen für die Nutzung des Virenfilters erfüllt sein:

- Installierte Antiviren-Lizenz. Nur mit installierter Lizenz ist das Menü „Antivirus“ aktiviert. Die Anleitung, wie Sie eine Lizenz anfordern und installieren, finden Sie im Abschnitt **Antivirus->Lizenzanforderung**.
- Zugriff auf einen Update-Server mit den aktuellen Versionen der Virensignaturen (siehe Abschnitt **Antivirus->Datenbank-Update**).
- Konfiguration und Aktivierung des Antiviren-Schutzes (siehe folgende Abschnitte für die jeweiligen Protokolle)

Ablauf der Antivirus-Lizenz

Wenn Ihre Antivirus-Lizenz abgelaufen ist, wird die weitere Aktualisierung der Virensignaturen gesperrt. Es erscheint im Menü Antivirus-Schutz Status->Datenbank-Update Status der Text „locked ([45] kavupdater licence expired)“. In diesem Fall können Sie nach dem Einspielen einer neuen Lizenz die Aktualisierung wieder freischalten, indem Sie **Unlock Database Update** im Menü Antivirus-Schutz Status anklicken.

Die Innominate AG behält sich vor, nach Ablauf Ihrer Antiviren-Lizenz im Zuge eines Software-Updates die Virensignaturen zu löschen, wenn aus Gründen der Speicherkapazität die Notwendigkeit dazu besteht (siehe „Update running“ auf Seite 48).

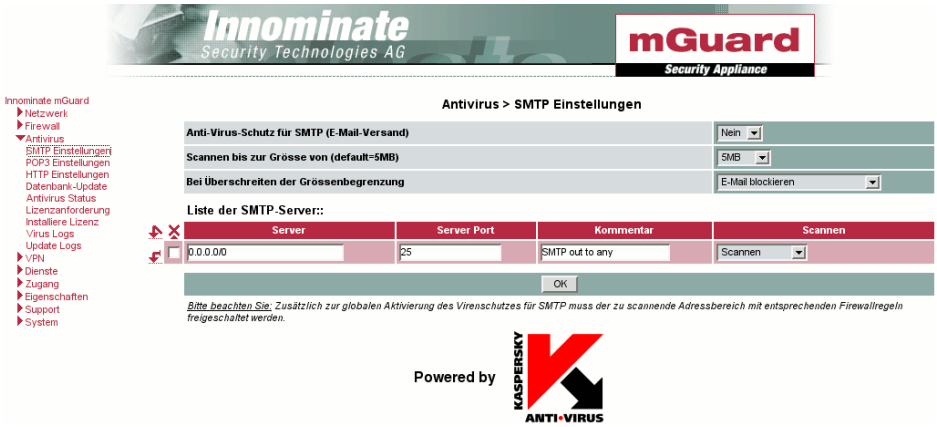
Dateigrößenbegrenzung

Durch die begrenzte Speicherkapazität des Innominate mGuard ergeben sich einige zu beachtende Unterschiede zu üblichen Virenfiltern.

Jede zu überprüfende Datei muß komplett auf die mGuard-RAM-Disk kopiert werden, damit sie durch den Virenfilter dekomprimiert und auf Viren untersucht werden kann. Da der Innominate mGuard mehrere Verbindungen gleichzeitig überwacht, um z.B. parallel E-Mail-Clients und Web-Browser nutzen zu können, kann es zu Speicher-Engpässen kommen. Um diesen Engpässen vorzubeugen, muss im Menü die Maximalgröße der zu überprüfenden Dateien festgelegt werden. Mit den voreingestellten Werten für die Maximalgröße ist in den meisten Szenarien ein problemloser Betrieb des Antivirenfilters möglich, deswegen sollten Sie diese Werte möglichst nicht ändern.

Sie können im Menü auswählen, ob bei einer Überschreitung der Maximalgröße die Nachricht blockiert und eine Fehlermeldung an Sie gesendet werden soll, oder ob die Datei ohne Virenüberprüfung weitergeleitet werden soll.

Antivirus → SMTP-Einstellungen



Das SMTP-Protokoll wird von Ihrem E-Mail-Client oder Mail-Transfer-Agent (MTA) zur Versendung von E-Mails genutzt.

☞ Der Virenfilter kann nur unverschlüsselte Daten auf Viren untersuchen. Deshalb sollten Sie Verschlüsselungsoptionen wie TLS nicht aktivieren. Im Falle des Erkennens eines Virus oder beim Auftreten von Fehlern wird der E-Mail-Client des Absenders durch einen Fehlercode benachrichtigt und ein Logeintrag im Antivirus-Log vorgenommen. Der ursprüngliche Empfänger erhält weder die infizierte Mail noch eine Benachrichtigung.

Anti-Virus-Schutz für SMTP (E-Mail-Versand)

Mit dieser Option aktivieren Sie den Virenfilter (Auf „Ja setzen) oder deaktivieren den Filter (Auf „Nein“ setzen). Bei einer Aktivierung wird eine Port-Redirection für SMTP-Verbindungen auf den SMTP-Proxy angelegt.

Scannen bis zur Grösse von (default=*x* MB)

Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an.

Wird diese Grenze überschritten, wird abhängig von der Einstellung „bei Überschreitung der Grössenbegrenzung“ eine Fehlermeldung an den E-Mail-Client zurückgegeben und die E-Mail nicht gesendet oder automatisch in den Durchlaßmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an den E-Mail-Client des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, das Versenden zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlaßmodus aktivieren.

Bitte beachten Sie, dass die Größe des Anhangs je nach Kodierung u.U. ein Vielfaches der ursprünglichen Datei sein kann.

Bei Überschreiten der Grössenbegrenzung

E-Mail ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlaßmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall wird nicht auf Viren überprüft!

E-Mail blockieren

Diese Option bewirkt die Ausgabe eines Fehlercodes an den E-Mail-Client und das Blockieren der E-Mail.

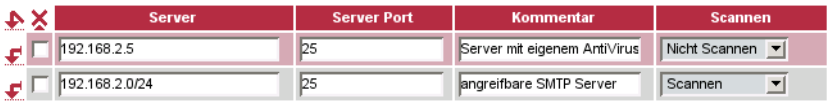
Liste der SMTP Server

Sie können die Server angeben, zu denen Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht.

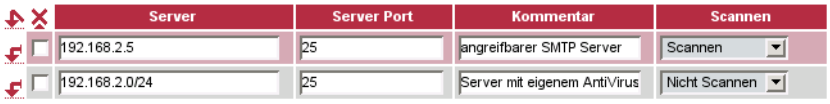
Beispiele:

Globale Aktivierung des Antivirus-Schutzes für SMTP:

Scan eines Subnetzes, Ausklammerung eines SMTP-Servers:



Scan für einen einzelnen SMTP-Server in einem Subnetz:



☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

⌧ Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.

⌧ Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.

⌧ Das Einschalten des SMTP Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr zu allen SMTP-Servern wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

⌧ Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der

Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das SMTP-Protokoll an. Der SMTP-Standardport **25** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

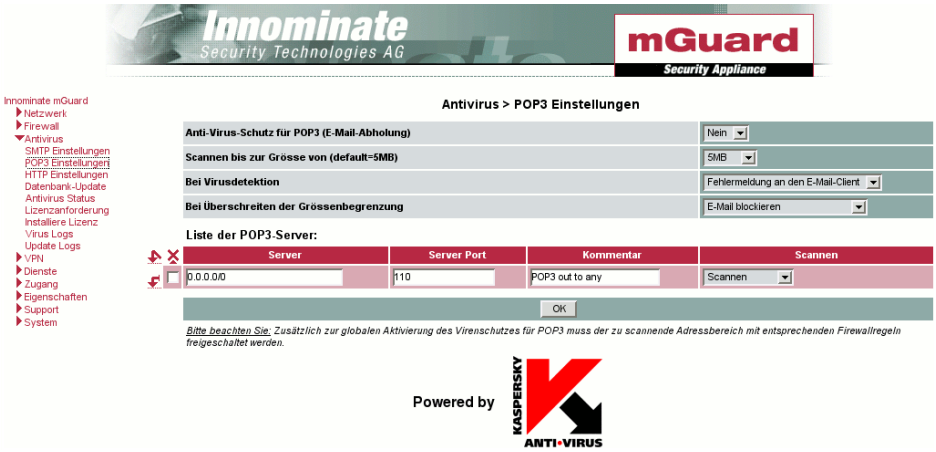
Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

Antivirus → POP3-Einstellungen



Das POP3-Protokoll wird von Ihrem E-Mail-Client zum Empfang von E-Mails genutzt

☞ Der Virenfilter kann nur unverschlüsselte Daten auf Viren untersuchen. Deshalb sollten Sie Verschlüsselungsoptionen wie STLS oder SSL nicht aktivieren. Die verschlüsselte Authentifizierung mittels AUTH ist dagegen nutzbar, da die eigentliche Übertragung der E-Mail unverschlüsselt erfolgt.

Anti-Virus-Schutz für POP3 (E-Mail-Abholung)

Mit dieser Option aktivieren Sie den Virenfilter (Auf „Ja“ setzen) oder deaktivieren den Filter (Auf „Nein“ setzen). Bei einer Aktivierung wird eine Port-Redirection für POP3-Verbindungen auf den POP3-Proxy angelegt.

⌦ Tip: Bei einer POP3-Verbindung werden durch die meisten E-Mail-Clients alle E-Mails über eine Verbindung abgerufen, so daß die neue Einstellung erst gilt, wenn die letzte Mail der aktuellen Verbindung von diesem Server abgerufen wurde. Um also während eines laufenden E-Mail-Transfers Einstellungen zu verändern, sollte der Transfer zunächst abgebrochen werden.

Scannen bis zur Grösse von (default=*x* MB)

Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an.
Wird diese Grenze überschritten, wird abhängig von der Einstellung „bei Überschreiten der Größenbegrenzung“ eine Fehlermeldung an den E-Mail-Client gesendet und die E-Mail nicht empfangen oder automatisch in den Durchlaßmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an den E-Mail Client des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, das Abholen der E-Mail zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlaßmodus aktivieren.

Bitte beachten Sie, dass die Größe des Anhangs je nach Kodierung u.U. ein Vielfaches der ursprünglichen Datei sein kann.

Bei Virusdetektion

Benachrichtigung per E-Mail
Erkennt der Virenfilter einen Virus, dann wird der Empfänger durch eine E-Mail benachrichtigt.

Fehlermeldung an den E-Mail Client
Erkennt der Virenfilter einen Virus, dann wird der Empfänger durch eine Fehlermeldung an den E-Mail-Client benachrichtigt.

☞ Ist für die E-Mail-Client-Software die Option „Gelesene E-Mails auf dem Server löschen“ aktiviert, so wird bei der Einstellung „Benachrichtigung per E-Mail“ die infizierte Mail auf dem Server gelöscht, da der E-Mail-Client davon ausgeht, daß die E-Mail erfolgreich übertragen wurde. Ist dies nicht gewünscht (wenn z.B. die infizierte E-Mail auf anderem Weg heruntergeladen werden soll), sollte ausschließlich die Option „Fehlermeldung an den E-Mail Client“ genutzt werden.

bei Überschreiten der Grössenbegrenzung

E-Mail ungescannt durchlassen
Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlaßmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall findet keine Überprüfung auf Viren statt!

E-Mail blockieren
Diese Option bewirkt die Ausgabe eines Fehlercodes an den E-Mail-Client und das Blockieren der E-Mail.

Liste der POP3 Server

Sie können die Server auswählen, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von „trusted“ Servern möglich.

Beispiele:
Globale Aktivierung des Antivirus-Schutzes für POP3:

Scan eines Subnetzes, Ausklammerung eines „trusted“ POP3-Servers:

Server	Server Port	Kommentar	Scannen
192.168.2.5	110	ungesichertes POP3	Nicht Scannen
192.168.2.0/24	110	gesichertes POP3	Scannen

Scan eines einzelnen „untrusted“ POP3 Servers in einem Subnetz:

Server	Server Port	Kommentar	Scannen
192.168.2.5	110	gesichertes POP3	Scannen
192.168.2.0/24	110	ungesichertes POP3	Nicht Scannen

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.
- Das Einschalten des POP3 Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller POP3-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

- Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das POP3-Protokoll an. Der POP3-Standardport **110** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

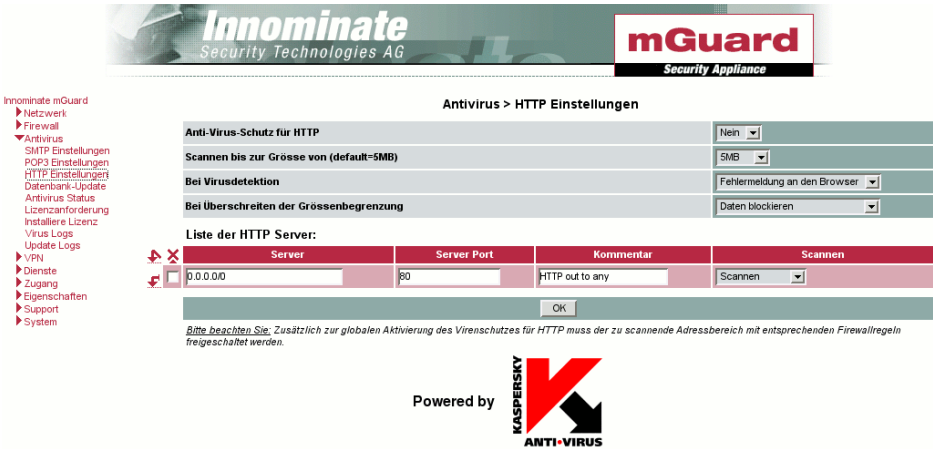
Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

Antivirus → HTTP-Einstellungen



Das HTTP-Protokoll wird von Web-Browsern zur Übertragung von Webseiten genutzt, hat aber noch viele andere Anwendungen. So wird es z.B. auch zum Download von Dateien wie z.B. Software-Updates oder zur Initialisierung von Multimedia-Streams genutzt.

Die Weiterleitung einer übertragenen Datei erfolgt erst, nachdem sie komplett geladen und überprüft wurde. Deshalb kann es bei größeren Dateien oder einer langsamen Download-Geschwindigkeit zu Verzögerungen in der Reaktionszeit der Benutzer-Software kommen.

⌧ Um den Anti-Virus-Schutz für HTTP zu testen, bietet sich zunächst der ungefährliche Eicar-Testvirus an, der eigens für Testzwecke unter der Adresse http://www.eicar.org/anti_virus_test_file.htm heruntergeladen werden kann.

Anti-Virus-Schutz für HTTP

Mit dieser Option aktivieren Sie den Virenfilter (Auf „Ja setzen) oder deaktivieren den Filter (Auf „Nein“ setzen). Bei einer Aktivierung wird eine Port-Redirection für SMTP-Verbindungen auf den HTTP-Proxy angelegt.

Scannen bis zur Grösse von (default=*x* MB)

Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an.

Wird diese Grenze überschritten, wird eine Fehlermeldung an den Browser gesendet oder automatisch in den Durchlaßmodus geschaltet.

Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software (Browser, Download-Manager) des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlaßmodus aktivieren.

Bei Virusdetektion

Fehlermeldung an den Browser

Erkennt der Virenfilter einen Virus innerhalb eines Datentransfers vom HTTP-Server zum HTTP-Client, dann wird eine Fehlermeldung an den HTTP-Client gesendet. Die Darstellung dieser Fehlermeldung hängt vom jeweiligen HTTP-Client ab. Ein Webbrowser wird die Fehlermeldung in Form einer HTML-Seite darstellen. Ist eine innerhalb einer HTML-Seite nachgeladene Datei - z.B. eine Bilddatei - infiziert, so wird diese Datei im Browser nicht angezeigt. Wird ein Dateidownload per HTTP mittels Download-Mana-

ger vorgenommen, so wird die Fehlermeldung im Download-Manager angezeigt.

Bei Überschreiten der Grössenbegrenzung

Daten ungescannt durchlassen
Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlaßmodus, wenn die eingestellte Dateigröße überschritten wird.

☞ In diesem Fall wird nicht auf Viren überprüft!

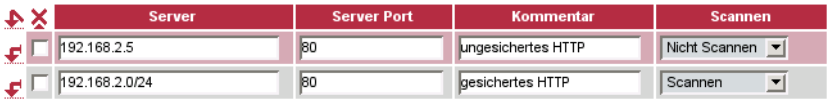
Daten blockieren
Diese Option bewirkt den Abbruch des Downloads und die Ausgabe eines Fehlercodes an die Client-Software.

Liste der HTTP Server

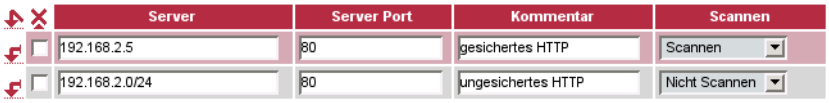
Sie können die Server auswählen, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von „trusted“ Servern möglich.

Beispiele:
Globale Aktivierung des Antivirus-Schutzes für HTTP:

Scan eines Subnetzes, Ausklammerung eines „trusted“ HTTP-Servers:



Scan eines einzelnen „untrusted“ HTTP-Servers in einem Subnetz:



☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

- Um den Anti-Virus-Schutz für HTTP- bzw. „FTP over HTTP“-Datenverkehr über einen Proxy zu aktivieren, fügen Sie eine neue Zeile in die Liste der Server ein und ersetzen den voreingestellten Port 80 durch den Proxy Port, welcher in Ihrem Webbrowser eingestellt ist.
  Gebräuchliche Proxy-Portnummern sind 3128 und 8080.
- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP-Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller HTTP-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

⌦ Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das HTTP-Protokoll an. Der HTTP-Standardport **80** ist bereits voreingestellt.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Scannen

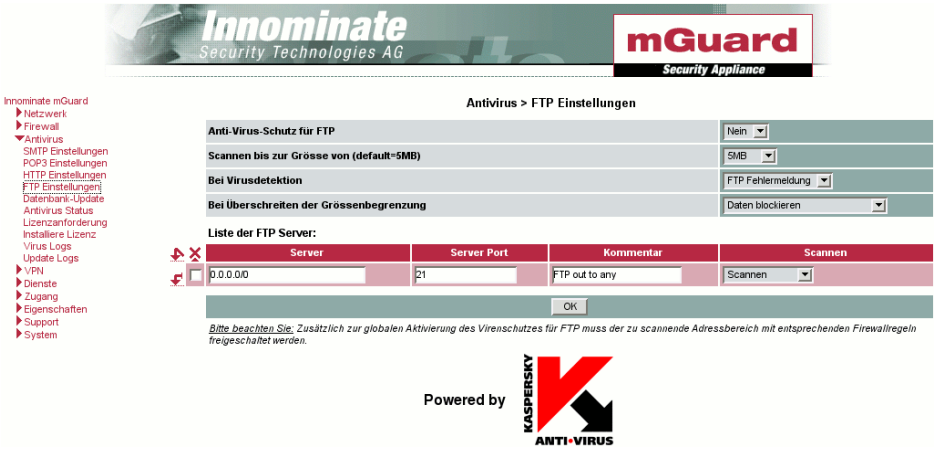
Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

Antivirus → FTP-Einstellungen



Das FTP-Protokoll wird zum Down oder Upload von Dateien genutzt.

☞ Die Weiterleitung einer übertragenen Datei erfolgt erst, nachdem sie komplett geladen und überprüft wurde. Deshalb kann es bei größeren Dateien oder einer langsamen Download-Geschwindigkeit zu Verzögerungen in der Reaktionszeit der Benutzer-Software kommen.

☞ Um den Anti-Virus-Schutz für FTP zu testen, bietet sich zunächst der ungefährliche Eicar-Testvirus an, der eigens für Testzwecke unter der Adresse ftp://ftp.kaspersky.com/utils/eicar/EICAR.COM heruntergeladen werden kann.

Anti-Virus-Schutz für FTP

Mit dieser Option aktivieren Sie den Virenfilter (Auf „Ja setzen) oder deaktivieren den Filter (Auf „Nein“ setzen). Bei einer Aktivierung wird eine Port-Redirection für FTP-Verbindungen auf den FTP-Proxy angelegt.

Scannen bis zur Grösse von (default=*x* MB)

Hier geben Sie die Maximalgröße der zu überprüfenden Dateien an.

Wird diese Grenze überschritten, wird eine Fehlermeldung an den Client gesendet oder automatisch in den Durchlaßmodus geschaltet.
Wenn die Speicherkapazität des mGuard nicht ausreicht, um die Datei vollständig zu speichern oder zu dekomprimieren, wird eine entsprechende Fehlermeldung an die Client-Software des Benutzers ausgegeben und ein Eintrag im Antivirus-Log vorgenommen. In diesem Fall haben Sie folgende Optionen:

- Sie können versuchen, den Download zu einem späteren Zeitpunkt zu wiederholen
- Sie können den Virenfilter für den betreffenden Server kurzzeitig deaktivieren
- Sie können die Option für den automatischen Durchlaßmodus aktivieren.

Bei Virusdetektion

FTP Fehlermeldung

Erkennt der Virenfilter einen Virus innerhalb eines Datentransfers vom FTP-Server zum FTP-Client, dann wird eine Fehlermeldung an den FTP-Client gesendet. Die Darstellung dieser Fehlermeldung hängt vom jeweiligen FTP-Client ab.

Bei Überschreiten der Grössenbegrenzung

Daten ungescannt durchlassen

Diese Option bewirkt ein automatisches Umschalten des Virenfilters in den Durchlaßmodus, wenn die eingestellte Dateigröße überschritten wird.

⌦ In diesem Fall wird nicht auf Viren überprüft!

Daten blockieren

Diese Option bewirkt den Abbruch des Downloads und die Ausgabe eines Fehlercodes an die Client-Software.

Liste der FTP Server

Sie können die Server auswählen, deren Datenverkehr gefiltert werden soll und für jede IP explizit angeben, ob der Antivirus-Schutz aktiviert werden soll oder nicht. Dadurch ist auch die Angabe von „trusted“ Servern möglich.

Beispiele:
Globale Aktivierung des Antivirus-Schutzes für FTP:

Server	Server Port	Kommentar	Scannen
0.0.0.0/0	21	alle ausgehenden Verbindun	Scannen

Scan eines Subnetzes, Ausklammerung eines „trusted“ FTP-Servers:

Server	Server Port	Kommentar	Scannen
192.168.2.5	21	ungesichertes FTP	Nicht Scannen
192.168.2.0/24	21	gesichertes FTP	Scannen

Scan eines einzelnen „untrusted“ FTP-Servers in einem Subnetz:

Server	Server Port	Kommentar	Scannen
192.168.2.5	21	gesichertes FTP	Scannen
192.168.2.0/24	21	ungesichertes FTP	Nicht Scannen

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

- Um den Anti-Virus-Schutz für FTP-Datenverkehr über einen Proxy zu aktivieren, fügen Sie eine neue Zeile in die Liste der Server ein und ersetzen den voreingestellten Port 21 durch den Proxy Port.
- Der Regelsatz wird wie bei der Angabe der Firewallregeln von oben nach unten abgearbeitet, die Reihenfolge der Regeln ist also ausschlaggebend für das Ergebnis.
- Der Virenfilter kann parallel nur eine begrenzte Anzahl gleichzeitiger Verbindungen zu Mail-, HTTP- und FTP Servern verarbeiten. Wird diese Zahl überschritten, dann wird jeder weitere Verbindungsversuch abgelehnt.
- Das Einschalten des FTP Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Bei den Angaben haben Sie folgende Möglichkeiten:

Server

0.0.0.0/0 bedeutet alle Adressen, d. h. der Datenverkehr aller FTP-Server wird gefiltert. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

- Da ein Verbindungswunsch zunächst durch den Proxy entgegengenommen wird, reagiert die Benutzersoftware bei einer Anfrage an einen nicht-existenten Server (z.B. falsche IP-Adresse) so, als ob die Serververbindung aufgebaut wird, aber keine Daten gesendet werden. Durch die genaue Angabe der Serveradressen in der Liste wird dieses Verhalten verhindert, da der Proxy nur Anfragen an die in der Liste angegebenen Adressen entgegennimmt.

Server Port

Hier geben Sie bitte die Nummer des Ports für das FTP-Protokoll an. Der FTP-Standardport **21** ist bereits voreingestellt.

- Das Einschalten des FTP Virenfilters öffnet die Firewall für die entsprechenden Ports unabhängig von zusätzlichen anderslautenden Firewall-Regeln.

Scannen

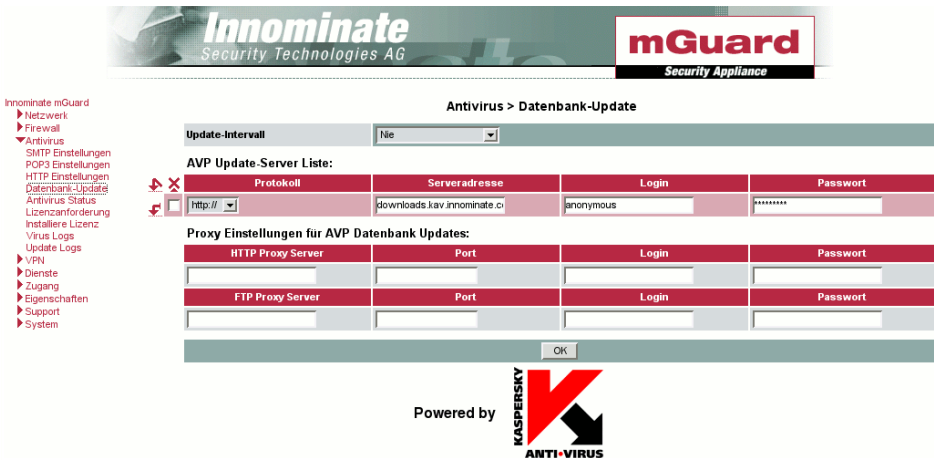
Scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server aktiviert.

Nicht scannen

Der Virenfilter ist für die in dieser Regel angegebenen Server deaktiviert.

Antivirus → Datenbank-Update



Die Virensignaturdateien können durch einen einstellbaren Update-Server in einem nutzerdefinierten Intervall aktualisiert werden. Das Update geschieht parallel zur Nutzung des Antivirenfilters. Im Auslieferungszustand befinden sich keine Virensignaturen auf dem mGuard. Deshalb sollte nach dem Aktivieren des

Antiviren-Schutzes mit der entsprechenden Lizenz auch das Update-Intervall eingestellt werden. Der Verlauf des Updates kann im Antivirus-Update-Log verfolgt werden.

Update-Intervall

Mit dieser Option wählen Sie das Aktualisierungsintervall der Signaturdateien. Die Größe der Datei beträgt z.Zt. etwa 3 MByte. Es werden nur die auf dem Update-Server aktualisierten Dateien nachgeladen.

AVP Update Server Liste:

Sie können die Server auswählen, von denen der Update der Virensignaturdatei geladen werden soll. Ein Standardserver ist bereits voreingetragen. Sie können bei Bedarf eigene Server angeben.

⌦ Die Liste der Server wird priorisiert von oben nach unten abgearbeitet, bis ein verfügbarer Server gefunden wurde.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Der Update der Virensignaturdateien kann entweder per FTP oder HTTP erfolgen.

Server Adresse

FQDN oder IP-Adresse des Servers inklusive des vollen Pfadnamens des Verzeichnisses, in der sich die Signaturdateien befinden.

Login

Login für den Server. Beim Update mittels HTTP-Protokoll ist eine Angabe des Logins u.U. nicht erforderlich.

Passwort

Passwort für den Login. Beim Update mittels HTTP-Protokoll ist eine Angabe des Logins u.U. nicht erforderlich.

Proxy Einstellungen für AVP Datenbank Updates:

Wenn der mGuard hinter einer Firewall ist, die HTTP oder FTP Verbindungen nur über einen Proxy Server erlaubt, können in den folgenden Zeilen die entsprechenden Proxies angegeben werden.

☞ Damit der Proxy Server verwendet wird müssen die Felder **HTTP** bzw. **FTP Proxy Server** *und* **Port** ausgefüllt sein.

☞ Damit eine Authentifizierung beim Proxy Server erfolgt müssen die Felder **Login** *und* **Passwort** ausgefüllt sein.

HTTP/FTP Proxy Server

Die IP oder der Hostname des Proxyservers.

Port

Der zu der IP oder dem Hostnamen gehörende Port des Proxyservers.

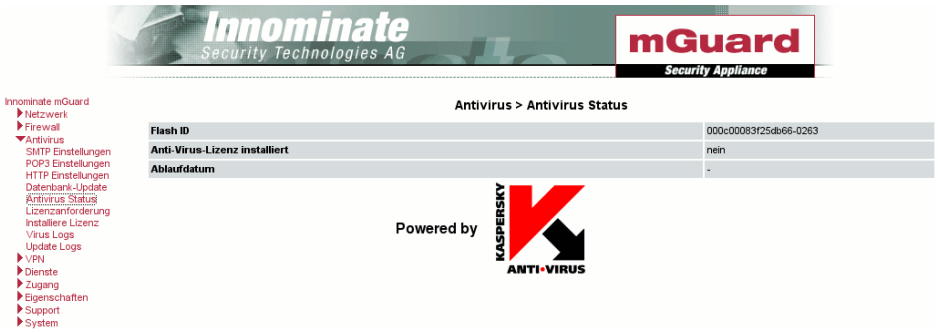
Login

Der Login, falls der Proxy Server eine Authentifizierung verlangt.

Passwort

Das zum Login gehörende Passwort.

Antivirus → Antivirus Status



Sie können die erfolgreiche Freischaltung des Virenfilters überprüfen. Unter diesem Menüpunkt finden Sie auch Informationen über das Ablaufdatum Ihrer Lizenz.

Antiviren-Schutz Status

Hier können Sie den Status der Scan-Engine überprüfen. Wenn die Überwachung für mindestens ein Protokoll aktiviert ist, wird hier der Status **up** angezeigt.

Letztes Datenbank-Update

Es wird der Tag angezeigt, an dem das letzte mal eine Änderung der Virensignaturen durchgeführt wurde.

Datenbank-Update Status

Hier wird angezeigt, ob die Datenbank-Aktualisierung aktiviert ist, ob gerade ein Datenbank-Update durchgeführt wird oder ob die Aktualisierung wegen einer abgelaufenen Antivirenlizenz gesperrt ist.

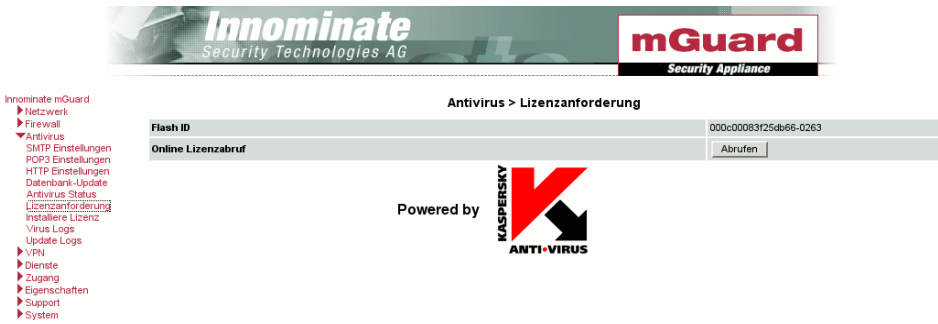
Antiviruslizenz installiert

Hier können Sie die Gültigkeit der installierten AVP-Lizenz überprüfen.

Ablaufdatum

Zeigt das Ablaufdatum der installierten AVP-Lizenz an.

Antivirus → Lizenzanforderung



Beim Kauf Ihrer Antivirus-Lizenz erhalten Sie einen Voucher, auf dem Sie ein Lizenz-Key und eine Lizenznummer finden. Um Ihren Virenfilter zu aktivieren, müssen Sie zunächst mit diesen Informationen Ihre Lizenzdatei anfordern. Dazu drücken Sie Abrufen im Menü **Antivirus->Lizenzanforderung**.

Sie gelangen dann auf eine Web-Seite, in deren Felder Sie die folgenden Informationen eingeben:

License Serial: Die Seriennummer, die auf Ihrem Vocher gedruckt ist

License Key: Der Lizenz-Key auf Ihrem Voucher

Flash Id: Wird automatisch vorausgefüllt

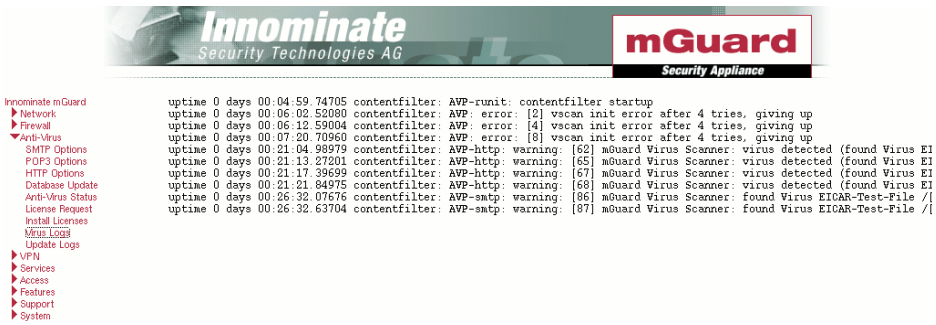
Email Address: Ihre E-Mail-Adresse für die Zustellung der Lizenzdatei

Nach erfolgreichem Ausfüllen des Formulars wird Ihnen die Lizenzdatei zugesendet.

Antivirus → Lizenzdatei installieren

Um die Lizenzdatei zu installieren, wählen Sie bitte die Datei im Menüpunkt **Antivirus->Installiere Lizenz** aus, um sie anschließend zu installieren.

Antivirus → Virus Logs


Innominate
Security Technologies AG
mGuard
Security Appliance
Innominate mGuard
Network
Firewall
Anti-Virus
SMTP Options
POP3 Options
HTTP Options
Database Update
Anti-Virus Status
License Request
Install Licenses
Virus Logs
Update Logs
VPN
Services
Access
Features
Support
System
uptime 0 days 00:04:59.74705 contentfilter: AVP-runit: contentfilter startup
uptime 0 days 00:06:02.52080 contentfilter: AVP: error: [2] vscan init error after 4 tries, giving up
uptime 0 days 00:06:12.59004 contentfilter: AVP: error: [4] vscan init error after 4 tries, giving up
uptime 0 days 00:07:20.70960 contentfilter: AVP: error: [8] vscan init error after 4 tries, giving up
uptime 0 days 00:21:04.98979 contentfilter: AVP-http: warning: [62] mGuard Virus Scanner: virus detected (found Virus EI
uptime 0 days 00:21:13.27201 contentfilter: AVP-http: warning: [65] mGuard Virus Scanner: virus detected (found Virus EI
uptime 0 days 00:21:17.39699 contentfilter: AVP-http: warning: [67] mGuard Virus Scanner: virus detected (found Virus EI
uptime 0 days 00:21:21.84975 contentfilter: AVP-http: warning: [68] mGuard Virus Scanner: virus detected (found Virus EI
uptime 0 days 00:26:32.07676 contentfilter: AVP-smtp: warning: [86] mGuard Virus Scanner: found Virus EICAR-Test-File /[
uptime 0 days 00:26:32.63704 contentfilter: AVP-smtp: warning: [87] mGuard Virus Scanner: found Virus EICAR-Test-File /[

Das Virus-Log enthält folgende Meldungen des Virenfilters:

- Gefundene Viren mit Angabe von Details (Name des Virus, Name der Datei, bei einer E-Mail zusätzlich: Absender, Datum, Betreff)
- Warnungen bei automatischer Einschaltung des Durchlaßmodus, wenn die zu filternde Datei die eingestellte Dateigröße überschreitet und nicht gefiltert wurde.
- Start und Fehlerausgaben der Kaspersky-Scan-Engine und des Virenfilters

Fehlermeldungen

Virus Detection

Ein Virus wurde erkannt. Die Fehlermeldung umfaßt den Namen des Virus, den Absender der E-Mail, das Absendedatum und den Namen der infizierten Datei bzw. den Namen der komprimierten Archivdatei und des infizierten Bestandteils dieses Archivs.
Beispiel einer Virenmeldung:

```
mGuard detected a virus. The mail could not be delivered.
found Virus Email-Worm.Win32.NetSky.q /[From
sick@example.com][Date Fri, 13 Aug 2004 11:33:53++0200]/
about_you.zip/document.txt.exe
[000012a7.00000077.00000000]
Message Details:
From: sick@example.com
Subject: Private document
Date: Fri, 13 Aug 2004 11:33:53 +0200
```

Exceeded maximum filesize

Die eingestellte Begrenzung der Dateigröße wurde überschritten.
Um die Datei trotzdem übertragen zu können, deaktivieren Sie für den Download den Virenfilter für den entsprechenden Server oder global. Alternativ können Sie den Durchlaßmodus (Menüpunkt: „bei Überschreiten der Größenbegrenzung) im jeweiligen Protokoll aktivieren.

⌧ In beiden Fällen wird die übertragene Datei nicht nach Viren untersucht!

Temporary Virus Scanner Failure

Ein temporärer Fehler trat bei dem Versuch auf, eine Datei zu scannen. Eine Wiederholung der Übertragung zu einem späteren Zeitpunkt oder ein Update der Virensignaturdatei kann evtl. das Problem beheben.
Mögliche Fehlerursachen:

- Die Scan-Engine ist nicht in der Lage, die Datei zu bearbeiten

- Die Speicherkapazität des Innominate mGuard reicht nicht zur Dekompression der Datei aus
- Interner Fehler der Scan-Engine

Exceptional Virus Scanner Failure

Ein Kommunikationproblem mit der Kaspersky-Scan-Engine trat auf. Genauere Angaben zum Problem finden Sie im Antivirus-Log.

Mögliche Fehlerursachen:

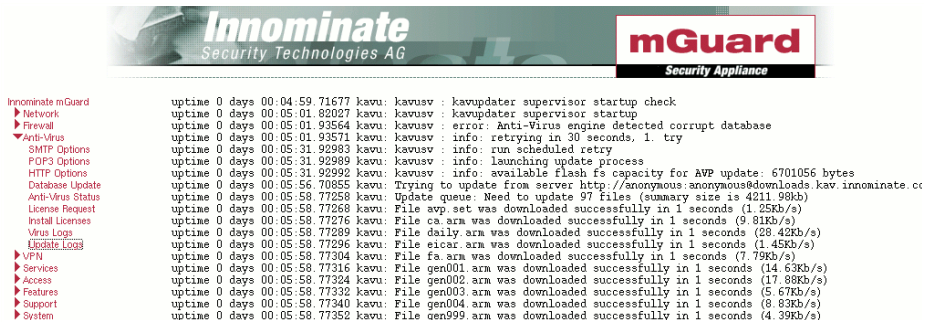
- Fehlgeschlagenes Signatur-Update durch fehlerhafte Angabe des Update-Servers (Menüpunkt Antivirus->Database Update)
- Ungültige oder veraltete Lizenz für den Virenfilter
- Beschädigtes oder fehlerhaftes Update der Virensignaturdatei

Update running

Der Virenfilter verfügt über keine Virensignaturen, der Download der Virensignaturen wurde bereits gestartet. Sie können den Fortschritt des Downloads im Menüpunkt Antivirus->Update Logs verfolgen.

Die Innominate AG behält sich vor, nach Ablauf Ihrer Antiviren-Lizenz im Zuge eines Software-Updates die Virensignaturen zu löschen, wenn aus Gründen der Speicherkapazität die Notwendigkeit dazu besteht. In diesem Fall erhalten Sie ebenfalls die Fehlermeldung „Update running“ beim Versuch der Benutzung des Virenfilters. Deaktivieren Sie in diesem Fall bitte den Virenfilter für alle Protokolle, um weiterhin ihren Email-Client bzw. Webbrowser nutzen zu können.

Antivirus → Update Logs


Innominate
Security Technologies AG
mGuard
Security Appliance
Innominate mGuard
Network
Firewall
Anti-Virus
SMTP Options
POP3 Options
HTTP Options
Database Update
Anti-Virus Status
License Request
Install Licenses
Virus Logs
Update Logs
VPN
Services
Access
Features
Support
System
uptime 0 days 00:04:59.71677 kavu: kavusv : kavupdater supervisor startup check
uptime 0 days 00:05:01.82027 kavu: kavusv : kavupdater supervisor startup
uptime 0 days 00:05:01.93564 kavu: kavusv : error: Anti-Virus engine detected corrupt database
uptime 0 days 00:05:01.93571 kavu: kavusv : info: retrying in 30 seconds, 1. try
uptime 0 days 00:05:31.92983 kavu: kavusv : info: run scheduled retry
uptime 0 days 00:05:31.92989 kavu: kavusv : info: launching update process
uptime 0 days 00:05:31.92992 kavu: kavusv : info: available flash fs capacity for AVP update: 6701056 bytes
uptime 0 days 00:05:56.70855 kavu: Trying to update from server http://anonymous:anonymous@downloads.kav.innominate.c
uptime 0 days 00:05:58.77258 kavu: Update queue: Need to update 97 files (summary size is 4211.98kb)
uptime 0 days 00:05:58.77268 kavu: File avp.set was downloaded successfully in 1 seconds (1.25Kb/s)
uptime 0 days 00:05:58.77276 kavu: File ca.arm was downloaded successfully in 1 seconds (9.81Kb/s)
uptime 0 days 00:05:58.77289 kavu: File daily.arm was downloaded successfully in 1 seconds (28.42Kb/s)
uptime 0 days 00:05:58.77296 kavu: File eicar.arm was downloaded successfully in 1 seconds (1.45Kb/s)
uptime 0 days 00:05:58.77304 kavu: File fa.arm was downloaded successfully in 1 seconds (7.79Kb/s)
uptime 0 days 00:05:58.77316 kavu: File gen001.arm was downloaded successfully in 1 seconds (14.63Kb/s)
uptime 0 days 00:05:58.77324 kavu: File gen002.arm was downloaded successfully in 1 seconds (17.88Kb/s)
uptime 0 days 00:05:58.77332 kavu: File gen003.arm was downloaded successfully in 1 seconds (5.67Kb/s)
uptime 0 days 00:05:58.77340 kavu: File gen004.arm was downloaded successfully in 1 seconds (8.83Kb/s)
uptime 0 days 00:05:58.77352 kavu: File gen999.arm was downloaded successfully in 1 seconds (4.39Kb/s)

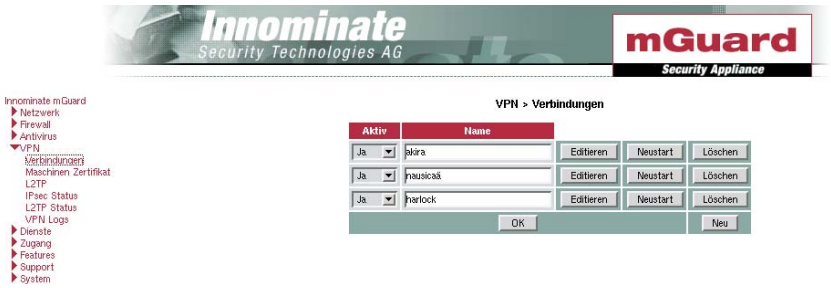
Das Update-Log enthält Meldungen über den Start und Verlauf des Update-Prozesses der Virensignaturdateien.

5.9 Menü VPN (nur enterprise)

Voraussetzungen für eine VPN-Verbindung:
Generelle Voraussetzung für eine VPN-Verbindung ist, dass die IP-Adressen der VPN-Partner bekannt und zugänglich sind.

- Damit eine IPsec-Verbindung erfolgreich aufgebaut werden kann, muss die VPN-Gegenstelle IPsec mit folgender Konfiguration unterstützen:
  – Authentifizierung über Pre-Shared Key (PSK) oder X.509 Zertifikate
  – ESP
  – Diffie-Hellman Gruppe 2 oder 5
  – DES, 3DES oder AES encryption
  – MD5 oder SHA-1 Hash Algorithmen
  – Tunnel oder Transport Modus
  – Quick Mode
  – Main Mode
  – SA Lifetime (1 Sekunde bis 24 Stunden)
  Ist die Gegenstelle ein Rechner unter Windows 2000, muss dazu das *Microsoft Windows 2000 High Encryption Pack* oder mindestens das *Service Pack 2* installiert sein.
- Befindet sich die Gegenstelle hinter einem NAT-Router, so muss die Gegenstelle NAT-T unterstützen. Oder aber der NAT-Router muss das IPsec-Protokoll kennen (IPsec/VPN Passthrough). In beiden Fällen sind aus technischen Gründen nur IPsec Tunnel-Verbindungen möglich.

VPN → Verbindungen



Listet die eingerichteten VPN-Verbindungen auf.

☞ Sie können jede einzelne Verbindung aktivieren (Aktiv = **Ja**) oder deaktivieren (Aktiv = **Nein**).

VPN-Verbindung löschen

☞ Klicken Sie neben dem betreffenden Eintrag **Löschen**.
Klicken Sie abschließend **OK**.

Neue VPN-Verbindung einrichten

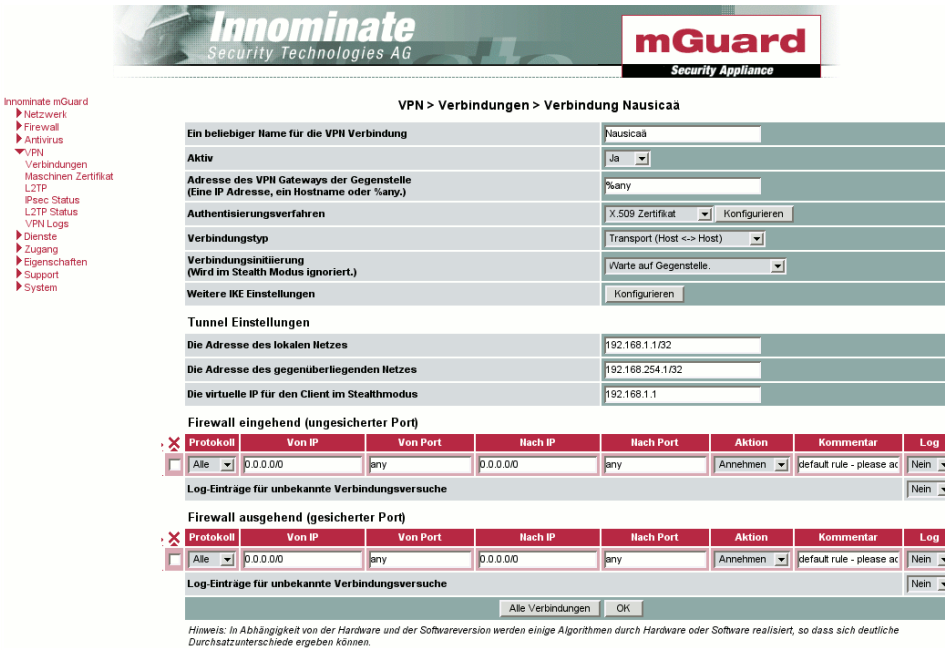
☞ Klicken Sie **Neu**.
Geben Sie der Verbindung einen Namen und klicken Sie **Editieren.**
Machen Sie die gewünschten bzw. erforderlichen Einstellungen (s. u.).
Klicken Sie abschließend **OK**.

VPN-Verbindung bearbeiten

☞ Klicken Sie neben der betreffenden Verbindung die Schaltfläche **Editieren**.
Machen Sie die gewünschten bzw. erforderlichen Einstellungen (s. u.).
Klicken Sie abschließend **OK**.

VPN-Verbindung neu starten

☞ Klicken Sie auf **Neustart** um die bestehende Verbindung zu beenden und erneut aufzubauen.



Ein beliebiger Name für die VPN Verbindung

Sie können die Verbindung frei benennen bzw. umbenennen.

Aktiv

Legen Sie fest, ob die Verbindung aktiv (= Ja) sein soll oder nicht (= Nein).

Adresse des VPN Gateways der Gegenstelle

Die Adresse des Übergangs zum privaten Netz, in dem sich der entfernte Kommunikationspartner befindet.

– Falls der mGuard aktiv die Verbindung zur entfernten Gegenstelle initiieren und aufbauen soll oder sich im *Stealth*-Modus befindet, dann geben Sie hier die IP-Adresse der Gegenstelle an. Statt einer IP-Adresse können Sie auch einen Hostnamen (d. h. Domain Namen im URL-Format in der Form vpn.example.com) eingeben.
– Falls der VPN Gateway der Gegenstelle keine feste und bekannte IP-Adresse hat, kann über die Inanspruchname des DynDNS-Service dennoch eine feste und bekannte Adresse simuliert werden. Siehe „Dienste → DynDNS Registrierung“ auf Seite 62.
– Falls der mGuard bereit sein soll, die Verbindung anzunehmen, die eine entfernte Gegenstelle mit beliebiger IP-Adresse aktiv zum lokalen mGuard initiiert und aufbaut, dann geben Sie an: **%any**
– Dann kann eine entfernte Gegenstelle den lokalen mGuard „anrufen“, die ihre eigene IP-Adresse (vom Internet Service Provider) dynamisch zugewiesen erhält, d. h. eine wechselnde IP-Adresse hat. Nur wenn in diesem Szenario die entfernte „anrufende“ Gegenstelle auch eine feste und bekannte IP-Adresse hat, können Sie diese IP-Adresse angeben.

⌦ **%any** kann nur zusammen mit dem Authentisierungsverfahren über X.509 Zertifikate verwendet werden.

⌦ Wenn sich die Gegenstelle hinter einem NAT Gateway befindet, muß **%any** gewählt werden. Ansonsten wird das Aushandeln weiterer Verbindungs-

schlüssel nach der ersten Kontaktaufnahme fehlschlagen.

Authentisierungsverfahren

Es gibt 2 Möglichkeiten:

– X.509 Zertifikat

– Pre-Shared Key

X.509 Zertifikat

Dieses Verfahren wird von den meisten neueren IPsec-Implementierungen unterstützt. Dabei verschlüsselt der mGuard die Authentifizierungs-Datagramme, die es zur Gegenstelle, dem „Tunnelende“ sendet, mit dem öffentlichen Schlüssel (Dateiname *.cer oder *.pem) der Gegenstelle. (Diese *.cer- oder *.pem-Datei haben Sie vom Bediener der Gegenstelle erhalten, z. B. per Diskette oder per E-Mail).

Um diesen öffentlichen Schlüssel dem mGuard zur Verfügung zu stellen, gehen Sie wie folgt vor:

Voraussetzung:

Sie haben die *.cer- oder *.pem-Datei auf dem Rechner gespeichert.

1. **Konfigurieren** klicken.
   Folge: Der Bildschirm *VPN > Verbindungen > Verbindung xyz > X.509 Zertifikat* erscheint. („*xyz*“ ist der jeweilige Name der Verbindung.)
2. **Durchsuchen...** klicken und die Datei selektieren.
3. **Importieren** klicken.
   Nach dem Import wird der Inhalt des neuen Zertifikats angezeigt - siehe nachfolgende Abbildung. Eine Erläuterung der angezeigten Informationen finden Sie im Kapitel „VPN → Maschinenzertifikat“ auf Seite 57.

4. **Zurück** klicken

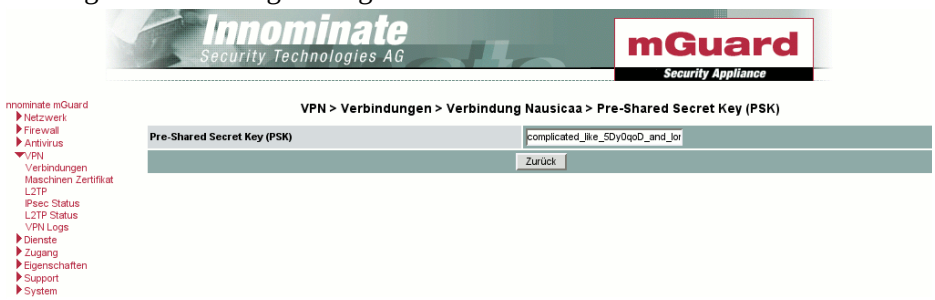
Pre-Shared Secret Key (PSK)

Dieses Verfahren wird vor allem durch ältere IPsec Implementierungen unterstützt. Dabei authentifizieren sich beide Seiten des VPNs über den gleichen PSK.

Um den verabredeten Schlüssel dem mGuard zur Verfügung zu stellen, gehen Sie wie folgt vor:

1. **Konfigurieren** klicken.

Folge: Der nachfolgend abgebildete Bildschirm erscheint.



2. Ins Eingabefeld *Pre-Shared Secret Key (PSK)* die verabredete Zeichenfolge eintragen. Um eine mit 3DES vergleichbare Sicherheit zu erzielen, sollte die Zeichenfolge aus ca. 30 nach dem Zufallsprinzip ausgewählten Klein- und Großbuchstaben sowie Ziffern bestehen.
3. **Zurück** klicken.

☞ *Pre-Shared Secret Key* kann nicht mit dynamischen (%any) IP-Adressen verwendet werden, nur feste IP-Adressen oder Hostnamen auf beiden Seiten werden unterstützt.

Verbindungstyp

Es stehen zur Auswahl:

- Tunnel (Netz ←→ Netz)
- Transport (Host ←→ Host)
- Transport (L2TP Microsoft Windows)
- Transport (L2TP SSH Sentinel)

Tunnel (Netz ←→ Netz)

Dieser Verbindungstyp eignet sich in jedem Fall und ist der sicherste. In diesem Modus werden die zu übertragenen IP-Datagramme vollkommen verschlüsselt und mit einem neuen Header versehen zur VPN-Gateway der Gegenstelle, dem „Tunnelende“, gesendet. Dort werden die übertragenen Datagramme entschlüsselt und aus ihnen die ursprünglichen Datagramme wiederhergestellt. Diese werden dann zum Zielrechner weitergeleitet.

Transport (Host ←→ Host)

Bei diesem Verbindungstyp werden nur die Daten der IP-Pakete verschlüsselt. Die IP Header Informationen bleiben unverschlüsselt.

Transport (L2TP Microsoft Windows)
Transport (L2TP SSH Sentinel)

Ist beim entfernten Rechner der Verbindungstyp IPsec/L2TP aktiviert, dann setzen Sie den mGuard auch auf *Transport (L2TP Microsoft Windows)* für ältere Microsoft Windows Versionen bzw. *Transport (SSH Sentinel)* für den SSH Sentinel Client oder neuere Microsoft Windows Versionen oder Service Packs.
Innerhalb der IPsec-Transport-Verbindung schafft das L2TP/PPP Protokoll einen Tunnel. Dem extern angeschlossenen IPsec/L2TP-Rechner wird seine IP-Adresse vom mGuard dynamisch zugewiesen.
Aktivieren Sie dazu auch den L2TP-Server des mGuards.

☞ Bei Verwendung eines Microsoft Windows Clients setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein** (siehe unten).

☞ Sobald unter Windows die IPsec/L2TP-Verbindung gestartet wird,

erscheint ein Dialogfeld, das nach Benutzername und Login fragt. Sie können dort beliebige Einträge machen, denn die Authentifizierung erfolgt bereits über die X.509 Zertifikate, so dass der mGuard diese Eingaben ignoriert.

Verbindungsinitiierung

Es gibt 2 Möglichkeiten:

- Starte die Verbindung zur Gegenstelle
- Warte auf Gegenstelle

Starte die Verbindung zur Gegenstelle

In diesem Fall initiiert der lokale mGuard die Verbindung zur Gegenstelle. Im Feld *Adresse des VPN Gateways der Gegenstelle* (s. o.) muss die feste IP-Adresse der Gegenstelle oder deren Domain Namen eingetragen sein.

Warte auf Gegenstelle

In diesem Fall ist der lokale mGuard bereit, die Verbindung anzunehmen, die eine entfernte Gegenstelle aktiv zum lokalen mGuard initiiert und aufbaut.

☞ Wenn Sie unter *Adresse des VPN Gateways der Gegenstelle* **%any** eingetragen haben, müssen Sie *Warte auf Gegenstelle* auswählen.

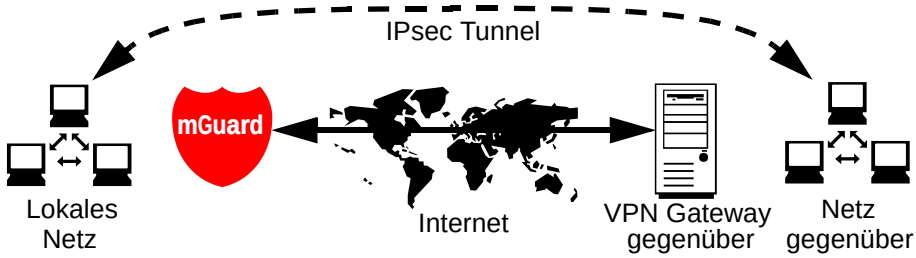
☞ Arbeitet der mGuard im *Stealth*-Modus, ist diese Einstellung wirkungslos. D. h. sie wird ignoriert und die Verbindung wird automatisch initiiert, wenn der mGuard bemerkt, dass die Verbindung genutzt werden soll.

Weitere IKE Einstellungen

Klicken Sie hier auf **Konfigurieren** wenn Sie Änderungen an den Einstellungen der Verschlüsselungsalgorithmen, Lebensdauer von Schlüssel oder Dead Peer Detection (DPD) vornehmen wollen. Eine ausführliche Erläuterung finden Sie unter „Weitere IKE Einstellungen“ auf Seite 55.

Tunnel Einstellungen

Wenn der *Verbindungstyp* auf „Tunnel“ gesetzt ist, müssen die folgenden Angaben gemacht werden:



Die Adresse des lokalen Netzes

Hier geben Sie die Adresse des Netzes oder Computers an, das lokal an den mGuard angeschlossen ist.

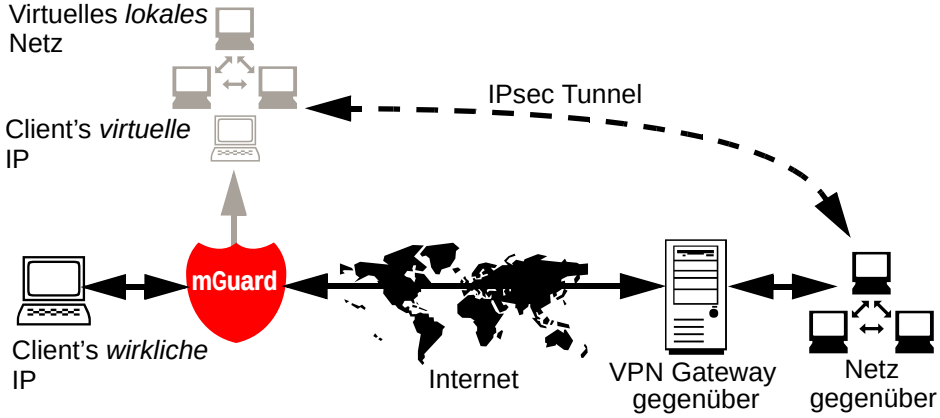
Die Adresse des gegenüberliegenden Netzes

Hier geben Sie die Adresse des Netzes oder Computers an, das sich hinter dem gegenüberliegenden VPN Gateway befindet.

☞ Die Adresse 0.0.0.0/0 gibt eine *Default Route über das VPN* an.

Das heißt, dass sämtlicher Datenverkehr, für den keine anderen Tunnel oder Routen existieren, durch diesen VPN Tunnel geleitet werden soll. Eine Default Route über das VPN sollte nur für einen Tunnel angegeben werden und kann im *Stealth* Modus nicht verwendet werden.

Die virtuelle IP für den Client im Stealth Modus



Im *Stealth*-Modus wird das lokale Netz des VPNs durch den mGuard simuliert. Innerhalb dieses *virtuellen* Netzes ist der Client unter einer *virtuellen* IP bekannt.

⌦ Dieser Eintrag wird nur im *Stealth*-Modus benötigt.

Firewall eingehend, Firewall ausgehend

Während die unter dem Menüpunkt *Firewall* vorgenommenen Einstellungen sich nur auf Nicht-VPN-Verbindungen beziehen (siehe oben unter „Firewall → Eingehend“ auf Seite 25), beziehen sich die Einstellungen hier ausschließlich auf die hier definierte VPN-Verbindung. Das bedeutet praktisch: Haben Sie mehrere VPN-Verbindungen definiert, können Sie für jede einzelne den Zugriff von außen oder von innen beschränken. Versuche, die Beschränkungen zu übergehen, können Sie ins Log protokollieren lassen.

⌦ Gemäß werksseitiger Voreinstellung ist die VPN-Firewall so eingestellt, dass für diese VPN-Verbindung alles zugelassen ist.
Für jede einzelne VPN-Verbindung gelten aber unabhängig voneinander gleichwohl die erweiterten Firewall-Einstellungen, die weiter oben definiert und erläutert sind - siehe „Firewall → Erweiterte Einstellungen“ auf Seite 31.

⌦ Sind mehrere Firewall-Regeln gesetzt, werden diese in der Reihenfolge der Einträge von oben nach unten abgefragt, bis eine passende Regel gefunden wird. Diese wird dann angewandt. Sollten nachfolgend in der Regelliste weitere Regeln vorhanden sein, die auch passen würden, werden diese ignoriert.

⌦ Im Stealth Modus ist in den Firewallregeln für den Client die wirkliche IP-Adresse zu verwenden oder aber auf 0.0.0.0/0 zu belassen, da nur ein Client durch den Tunnel angesprochen werden kann.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll

Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

Von IP/Nach IP

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

Von Port/Nach Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat Abweisen dieselbe Wirkung wie Verwerfen (s. u.).)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

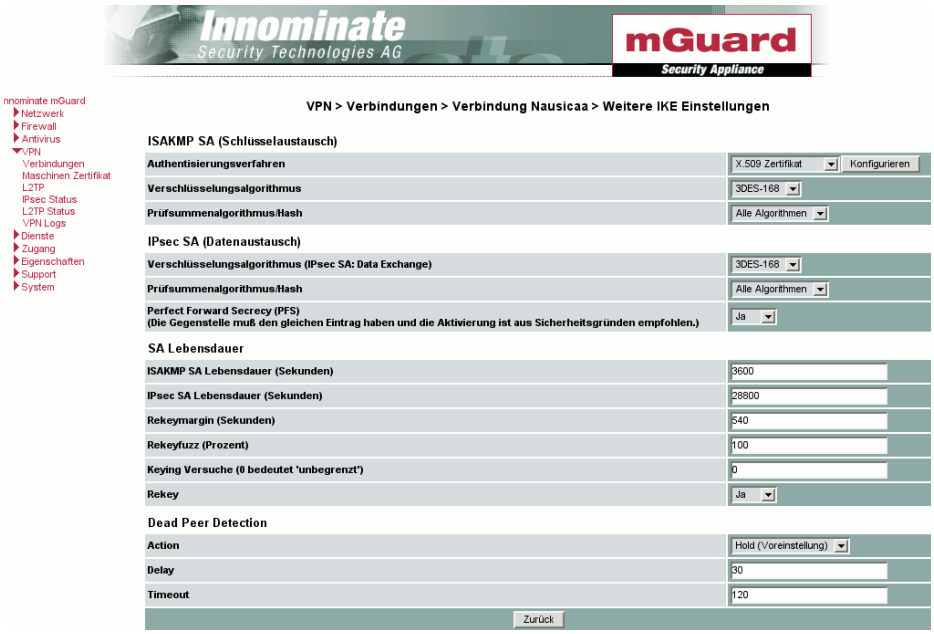
☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen

☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

Weitere IKE Einstellungen



ISAKMP SA (Schlüsselaustausch)

Verschlüsselungsalgorithmus

☞ Vereinbaren Sie mit dem Administrator der Gegenstelle, welches Verschlüsselungsverfahren verwendet werden soll.

3DES-168 ist das am häufigsten benutzte Verfahren und ist deshalb als Standard voreingestellt.

Grundsätzlich gilt Folgendes: Je mehr Bits ein Verschlüsselungsalgorithmus hat - angegeben durch die angefügte Zahl -, desto sicherer ist er. Das relativ neue Verfahren AES-256 gilt daher als am sichersten, ist aber noch nicht so verbreitet.

Der Verschlüsselungsvorgang ist um so zeitaufwendiger, je länger der Schlüssel ist. Dieser Gesichtspunkt spielt für den mGuard keine Rolle, weil er mit Hardware-basierter Verschlüsselungstechnik arbeitet. Jedoch könnte dieser Aspekt für die Gegenstelle eine Rolle spielen.

Der zur Auswahl stehende mit „Null“ bezeichnete Algorithmus beinhaltet keinerlei Verschlüsselung.

Prüfsummenalgorithmus/Hash

Lassen Sie die Einstellung auf *Alle Algorithmen* stehen. Dann spielt es keine Rolle, ob die Gegenstelle mit MD5 oder SHA-1 arbeitet.

IPsec SA (Datenaustausch)

Im Unterschied zu *ISAKMP SA (Schlüsselaustausch)* (s. o.) wird hier das Verfahren für den Datenaustausch festgelegt. Die können sich von denen des Schlüsselaustauschs unterscheiden, müssen aber nicht.

Verschlüsselungsalgorithmus

Siehe oben.

Prüfsummenalgorithmus/Hash

Siehe oben.

Perfect Forward Secrecy (PFS)

Verfahren zur zusätzlichen Steigerung der Sicherheit bei der Datenübertragung. Bei IPsec werden in bestimmten Intervallen die Schlüssel für den Datenaustausch erneuert. Mit PFS werden dabei mit der Gegenstelle neue Zufallszahlen ausgehandelt, anstatt sie aus zuvor verabredeten Zufallszahlen abzuleiten.

☞ Nur wenn die Gegenstelle PFS unterstützt, wählen Sie **Ja**.

Bei Auswahl des Verbindungstyps *Transport (L2TP Microsoft Windows)* setzen Sie *Perfect Forward Secrecy (PFS)* auf **Nein**.

SA Lebensdauer

Die Schlüssel einer IPsec Verbindung werden in bestimmten Abständen erneuert um die Kosten eines Angriffs auf eine IPsec Verbindung zu erhöhen.

ISAKMP SA Lebensdauer

Lebensdauer der für die ISAKMP SA vereinbarten Schlüssel in Sekunden. Die Werkseinstellung sind 3600 Sekunden (1 Stunde). Das erlaubte Maximum sind 28800 Sekunden (8 Stunden).

IPsec SA Lebensdauer

Lebensdauer der für die IPsec SA vereinbarten Schlüssel in Sekunden.

Die Werkseinstellung sind 28800 Sekunden (8 Stunden). Das erlaubte Maximum sind 86400 Sekunden (24 Stunden).

Rekey Margin

Minimale Zeitspanne vor Ablauf der alten Schlüssel, innerhalb der ein neuer Schlüssel erzeugt werden soll. Die Werkseinstellung sind 540 Sekunden (9 Minuten).

Rekeyfuzz

Maximum in Prozent, um das *Rekey Margin* zufällig vergrößert werden soll. Dies dient dazu den Schlüsselaustausch auf Maschinen mit vielen VPN Verbindungen zu zeitversetzt stattfinden zu lassen. Die Werkseinstellung sind 100 Prozent.

Keying Versuche

Anzahl der Versuche, die unternommen werden sollen, neue Schlüssel mit der Gegenstelle zu vereinbaren.

Der Wert 0 bedeutet bei Verbindungen, die der mGuard initiieren soll, unendlich viele Versuche, ansonsten 5 Versuche.

Rekey

Wenn auf **Ja**, dann wird diese Seite versuchen einen neuen Schlüssel zu vereinbaren wenn der alte abläuft.

Dead Peer Detection

Wenn die Gegenstelle Dead Peer Detection (DPD) Protokoll unterstützt, können die jeweiligen Partner erkennen, ob die IPsec Verbindung noch gültig ist oder nicht und evtl. neu aufgebaut werden muss.

Ohne DPD muß je nach Konfiguration bis zum Ablauf der SA Lebensdauer gewartet werden oder die Verbindung manuell neu initiiert werden.

Action

Bei **Hold** (Halten) wird versucht die IPsec Verbindung neu aufzubauen wenn diese für tod erklärt wurde. Bei **Clear** (Löschen) wird nicht versucht die Verbindung erneut aufzubauen.

Die Werkseinstellung ist **Hold**.

Delay

Zeitspanne in Sekunden nach welcher DPD Keep Alive Anfragen gesendet werden sollen, die testen ob die Gegenstelle noch verfügbar ist.

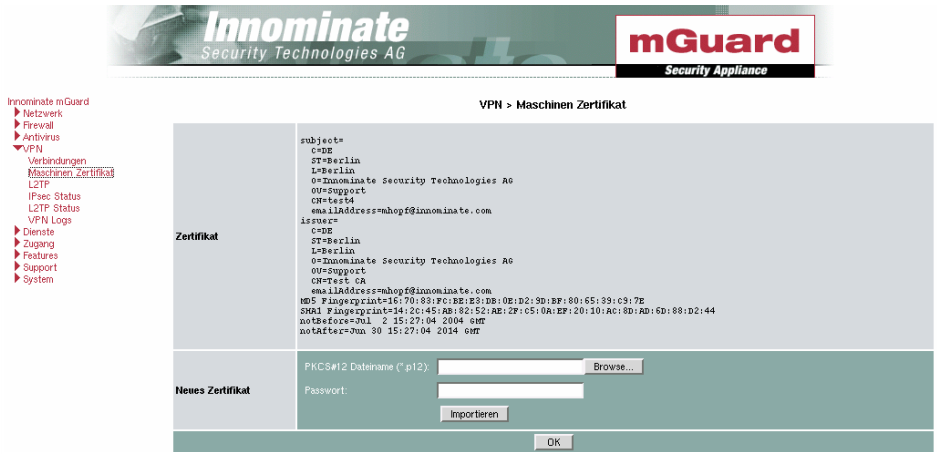
Die Werkseinstellung sind 30 Sekunden.

Timeout

Zeitspanne in Sekunden, nach der die Gegenstelle die Verbindung für tod erklärt werden soll, wenn auf die Keep Alive Anfragen keine Antwort erfolgte.

Die Werkseinstellung sind 120 Sekunden.

VPN → Maschinenzertifikat



Zertifikat

Zeigt das aktuell importierte X.509-Zertifikat an, mit dem sich der mGuard gegenüber anderen VPN-Gateways ausweist. Folgende Informationen werden angezeigt:

subject	Der Besitzer, auf den das Zertifikat ausgestellt ist.

issuer	Die Beglaubigungsstelle, die das Zertifikat unterschrieben hat. C : Land (Country) ST: Bundesland (State) L : Stadt (Location) O : Organisation OU: Abteilung (Organisation Unit) CN: Hostname, allgemeiner Name (Common Name)
MD5, SHA1 Fingerprint	Fingerabdruck des Zertifikats, um diesen z. B. am Telefon mit einem anderen zu vergleichen. Windows zeigt an dieser Stelle den Fingerabdruck im SHA1-Format an.
notBefore, notAfter	Gültigkeitszeitraum des Zertifikats. Wird vom mGuard mangels einer eingebauten Uhr ignoriert.

Die importierte Zertifikatsdatei (Dateinamen-Erweiterung *.p12 oder *.pfx) enthält neben den oben angegebenen Informationen die beiden Schlüssel, den öffentlichen zum Verschlüsseln, den privaten zum Entschlüsseln. Der zugehörige öffentliche Schlüssel kann an beliebig viele Verbindungspartner vergeben werden, so dass diese verschlüsselte Daten senden können.
In Abhängigkeit von der Gegenstelle muss das Zertifikat als .cer- oder .pem-Datei dem Bediener der entfernten Gegenstelle zur Verfügung gestellt werden - z. B. durch persönliche Übergabe oder per E-Mail. Wenn Ihnen kein sicherer Übertragungsweg zur Verfügung steht, sollten Sie anschließend den vom mGuard angezeigten Fingerabdruck über einen sicheren Weg vergleichen.

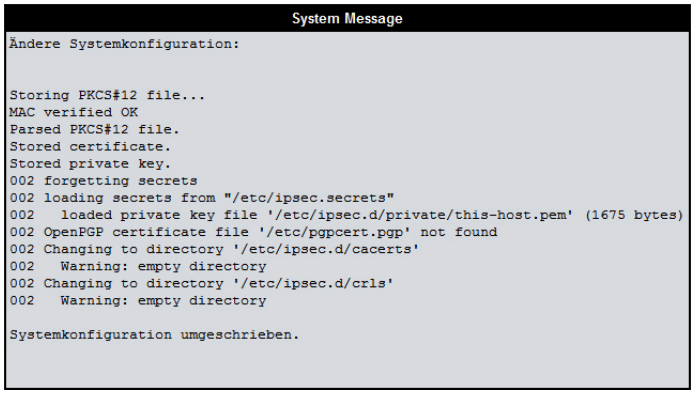
Es kann nur eine Zertifikats-Datei (PKCS#12-Datei) ins Gerät importiert werden.
Um ein (neues) Zertifikat zu importieren, gehen Sie wie folgt vor:

Neues Zertifikat

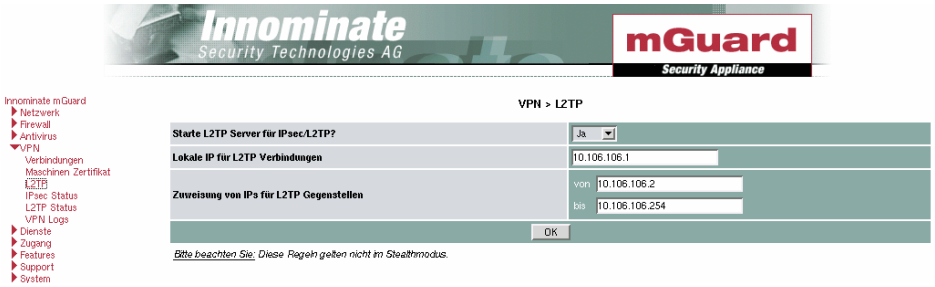
Voraussetzung:

Die Zertifikatsdatei (Dateiname = *.p12 oder *.pfx) ist generiert und auf dem angeschlossenen Rechner gespeichert.

1. **Durchsuchen...** klicken, um die Datei zu selektieren
2. In das Feld *Passwort* geben Sie das Passwort ein, mit dem der private Schlüssel der PKCS#12-Datei geschützt ist.
3. **Importieren** klicken.
4. Abschließend **OK** klicken.
   Nach dem Import erhalten Sie eine Systemmeldung:



VPN → L2TP



Start L2TP Server für IPsec/L2TP? Ja / Nein

Wollen Sie IPsec/L2TP-Verbindungen ermöglichen, setzen Sie diesen Schalter auf **Ja**.

Über IPsec können dann zum mGuard L2TP Verbindungen aufgebaut werden, über welche den Clients dynamisch IP Adressen innerhalb des VPNs zugeteilt werden.

Lokale IP für L2TP Verbindungen

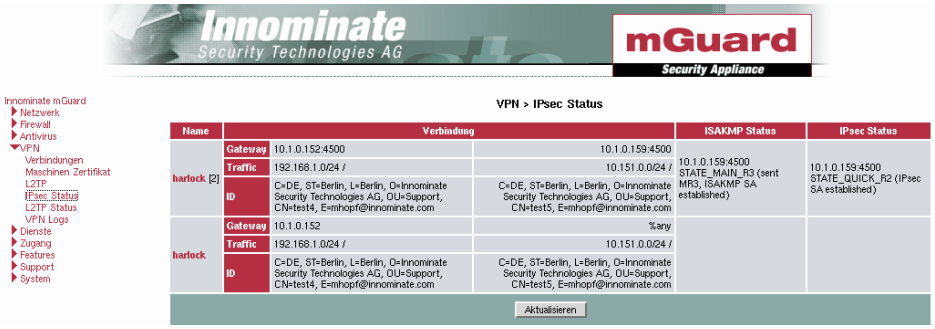
Nach dem obigen Screenshot teilt der mGuard der Gegenstelle mit, er habe die Adresse 10.106.106.1.

Zuweisung von IPs für L2TP Gegenstellen

Nach dem obigen Screenshot teilt der mGuard der Gegenstelle eine IP Adresse zwischen 10.106.106.2 und 10.106.106.254 mit.

VPN → IPsec Status

Nur Anzeige



Informiert über den Status der IPsec-Verbindungen.
Links sind die Namen der VPN-Verbindungen aufgelistet, rechts daneben wird jeweils deren aktueller Status angezeigt.

GATEWAY

zeigt die IP Adressen der miteinander kommunizierenden VPN Gateways

TRAFFIC

bezeichnet Rechner bzw. Netze, die über die VPN-Gateways kommunizieren.

ID

bezeichnet den Distinguished Name (DN) eines X.509-Zertifikats.

ISAKMP Status

ISAKMP Status (Internet security association and key management protocol) ist mit „established“ angegeben, wenn die beiden beteiligten VPN-Gateways einen Kanal zum Schlüsselaustausch aufgebaut haben. In diesem Fall konnten sie einander kontaktieren, und alle Einträge bis einschließlich „ISAKMP SA“ auf der Konfigurationsseite der Verbindung waren korrekt.

IPsec Status

IPsec Status ist mit „established“ angegeben, wenn die IPsec-Verschlüsselung bei der Kommunikation aktiviert ist. In diesem Fall waren auch die Angaben unter „IPsec SA“ und „Tunnel-Einstellungen“ korrekt.

Bei Problemen empfiehlt es sich, in die VPN-Logs des Rechners zu schauen, zu dem die Verbindung aufgebaut wurde. Denn der initiierende Rechner bekommt aus Sicherheitsgründen keine ausführlichen Fehlermeldungen zugesandt.

Falls angezeigt wird:

ISAKMP SA established, IPsec State: WAITING

Dann bedeutet das:

Die Authentifizierung war erfolgreich, jedoch stimmten die anderen Parameter nicht: Stimmt der Verbindungstyp (Tunnel, Transport) überein? Wenn Tunnel gewählt ist, stimmen die Netzbereiche auf beiden Seiten überein?

Falls angezeigt wird:

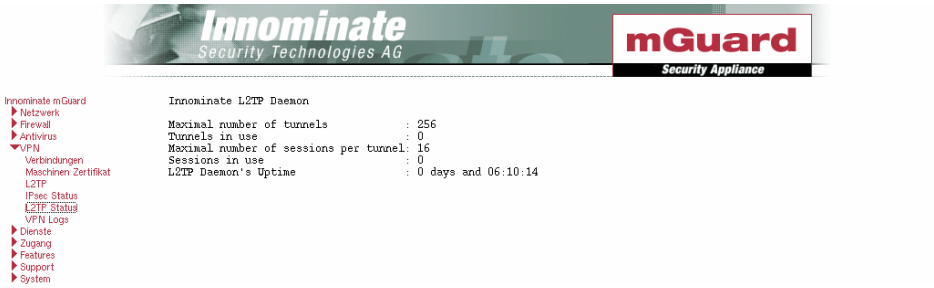
IPsec State: IPsec SA established

Dann bedeutet das:

Die VPN-Verbindung ist erfolgreich aufgebaut und kann genutzt werden. Sollte dies dennoch nicht der Fall sein, dann gibt es Probleme mit dem VPN-Gateway der Gegenstelle. In diesem Fall die Verbindung deaktivieren und wieder aktivieren, um die Verbindung erneut aufzubauen.

VPN → L2TP Status

Nur Anzeige

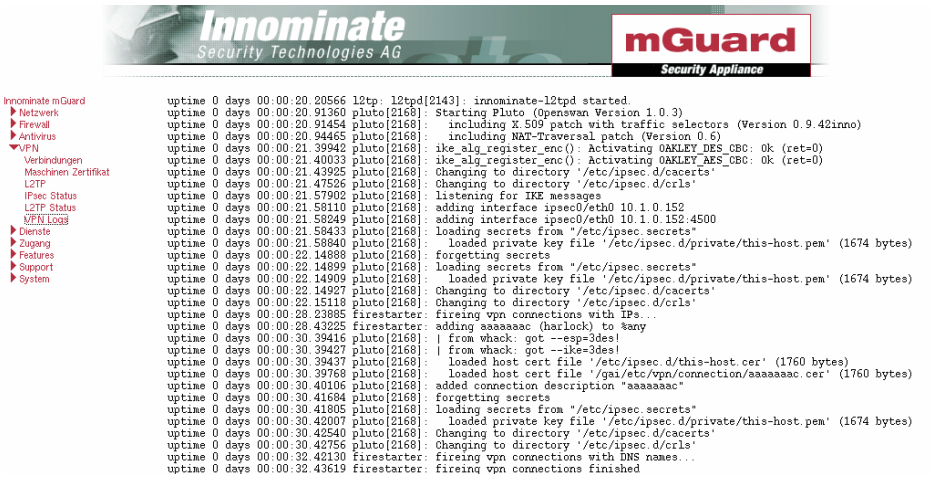


Informiert über den L2TP-Status, wenn dieser als Verbindungstyp gewählt ist. Siehe „VPN → Verbindungen“ auf Seite 49.

Ist dieser Verbindungstyp nicht gewählt, sehen Sie die abgebildete Anzeige.

VPN → VPN Logs

Nur Anzeige


Innominate
Security Technologies AG
mGuard
Security Appliance
Innominate mGuard
Netzwerk
Firewall
Antivirus
VPN
Verbindungen
Maschinen Zertifikat
L2TP
IPsec Status
L2TP Status
VPN Logs
Dienste
Zugang
Features
Support
System
uptime 0 days 00:00:20.20566 l2tp: l2tpd[2143]: innominate-l2tpd started.
uptime 0 days 00:00:20.91360 pluto[2168]: Starting Pluto (Openswan Version 1.0.3)
uptime 0 days 00:00:20.91454 pluto[2168]: including X.509 patch with traffic selectors (Version 0.9.42inno)
uptime 0 days 00:00:20.94465 pluto[2168]: including NAT-Traversal patch (Version 0.6)
uptime 0 days 00:00:21.39942 pluto[2168]: ike_alg_register_enc(): Activating OAKLEY_DES_CBC: Ok (ret=0)
uptime 0 days 00:00:21.40033 pluto[2168]: ike_alg_register_enc(): Activating OAKLEY_AES_CBC: Ok (ret=0)
uptime 0 days 00:00:21.43925 pluto[2168]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:21.47526 pluto[2168]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:00:21.57902 pluto[2168]: listening for IKE messages
uptime 0 days 00:00:21.58110 pluto[2168]: adding interface ipsec0/eth0 10.1.0.152
uptime 0 days 00:00:21.58249 pluto[2168]: adding interface ipsec0/eth0 10.1.0.152:4500
uptime 0 days 00:00:21.58433 pluto[2168]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:21.58840 pluto[2168]: loaded private key file '/etc/ipsec.d/private/this-host.pem' (1674 bytes)
uptime 0 days 00:00:22.14888 pluto[2168]: forgetting secrets
uptime 0 days 00:00:22.14899 pluto[2168]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:22.14909 pluto[2168]: loaded private key file '/etc/ipsec.d/private/this-host.pem' (1674 bytes)
uptime 0 days 00:00:22.14927 pluto[2168]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:22.15118 pluto[2168]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:00:28.23885 firestarter: fireing vpn connections with IPs...
uptime 0 days 00:00:28.43225 firestarter: adding aaaaaaac (harlock) to %any
uptime 0 days 00:00:30.39416 pluto[2168]: | from whack: got --esp=3des!
uptime 0 days 00:00:30.39427 pluto[2168]: | from whack: got --ike=3des!
uptime 0 days 00:00:30.39437 pluto[2168]: loaded host cert file '/etc/ipsec.d/this-host.cer' (1760 bytes)
uptime 0 days 00:00:30.39768 pluto[2168]: loaded host cert file '/gai/etc/vpn/connection/aaaaaaac.cer' (1760 bytes)
uptime 0 days 00:00:30.40106 pluto[2168]: added connection description "aaaaaaac"
uptime 0 days 00:00:30.41684 pluto[2168]: forgetting secrets
uptime 0 days 00:00:30.41805 pluto[2168]: loading secrets from "/etc/ipsec.secrets"
uptime 0 days 00:00:30.42007 pluto[2168]: loaded private key file '/etc/ipsec.d/private/this-host.pem' (1674 bytes)
uptime 0 days 00:00:30.42540 pluto[2168]: Changing to directory '/etc/ipsec.d/cacerts'
uptime 0 days 00:00:30.42756 pluto[2168]: Changing to directory '/etc/ipsec.d/crls'
uptime 0 days 00:00:32.42130 firestarter: fireing vpn connections with DNS names...
uptime 0 days 00:00:32.43619 firestarter: fireing vpn connections finished

Listet alle VPN-Ereignisse auf.

Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

5.10 Menü Dienste

Dienste → DNS

Soll der mGuard eine Verbindung zu einer Gegenstelle aufbauen (z. B. VPN-Gateway oder NTP-Server), muss ihm die IP-Adresse dieser Gegenstelle bekannt sein. Wird ihm die Adresse in Form eines Hostnamens angegeben (d. h. in der Form www.example.com), dann muss das Gerät auf einem Domain Name Server (DNS) nachschlagen, welche IP-Adresse sich hinter dem Hostnamen verbirgt.
Wenn sich der mGuard nicht im *Stealth*-Modus befindet, können Sie die lokal angeschlossenen Clients so konfigurieren, dass sie den mGuard zur Auflösung von Hostnamen in IP-Adressen benutzen können. Siehe „IP-Konfiguration bei Windows-Clients“ auf Seite 66

Hostnamen Modus

Mit *Hostnamen Modus* und *Hostname* können Sie dem mGuard einen Namen geben. Dieser wird dann z. B. beim Einloggen per SSH angezeigt. Eine Namensgebung erleichtert die Administration mehrerer mGuards.

Nutzer definiert (siehe unten)

(Standard) Der im Feld *Hostname* eingetragene Name wird als Name für den mGuard gesetzt.

☞ Arbeitet der mGuard im *Stealth*-Modus, muss als *Hostnamen Modus* die Option *Nutzer definiert* gewählt werden.

Provider definiert (z. B. via DHCP)

Wenn der Netzwerkmodus ein externes Setzen des Hostnamens erlaubt wie z. B. bei DHCP, dann wird der vom Provider übermittelte Name für den mGuard gesetzt.

Hostname

Ist unter *Hostnamen Modus* die Option *Nutzer definiert* ausgewählt, dann tragen Sie hier den Namen ein, den der mGuard erhalten soll.

Sonst, d. h. wenn unter *Hostnamen Modus* die Option *Provider definiert (z. B. via DHCP)* ausgewählt ist, wird ein Eintrag in diesem Feld ignoriert.

Domain-Suchpfad

Erleichtert dem Benutzer die Eingabe eines Domain-Namens: Gibt der Benutzer den Domain-Name gekürzt ein, ergänzt der mGuard seine Eingabe um den angegebenen Domain-Suffix, der hier unter *Domain-Suchpfad* festgelegt wird.

Benutzte Nameserver

Möglichkeiten:

- Root Nameserver
- Provider definiert
- Nutzer definiert

Root Nameserver:
Anfragen werden an die Root-Nameserver im Internet gerichtet, deren IP-Adressen im mGuard gespeichert sind. Diese Adressen ändern sich selten.

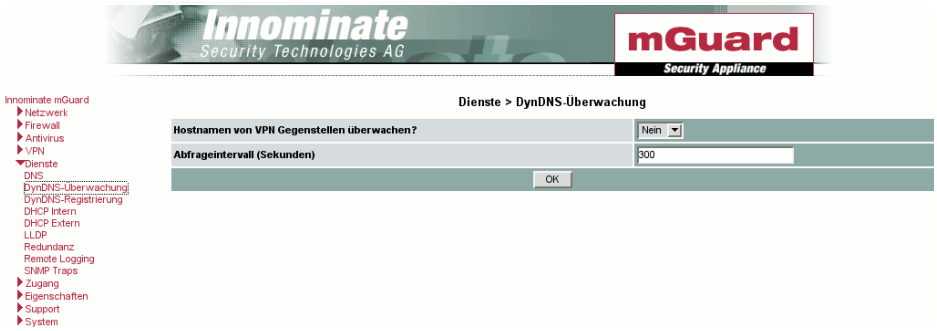
Provider definiert (z. B. via PPPoE oder DHCP)
Es wird der Domain Name Server des Internet Service Providers benutzt, der den Zugang zum Internet zur Verfügung stellt. Wählen Sie diese Einstellung nur wenn der mGuard im *PPPoE*-, im *PPTP*-Modus oder im *Router*-Modus mit DHCP arbeitet.

Nutzer definiert (unten stehende Liste)
Ist diese Einstellung gewählt, nimmt der mGuard mit den Domain Name Servern Verbindung auf, die in der Liste *Nutzer definierte Nameserver* aufgeführt sind.

Nutzer definierter Nameserver
In dieser Liste können Sie die IP-Adressen von Domain Name Servern erfassen. Soll einer von diesen vom mGuard benutzt werden, wählen Sie unter **Benutzte Nameserver** die Option *Nutzer definiert (unten stehende Liste)* fest.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Dienste → DynDNS Überwachung

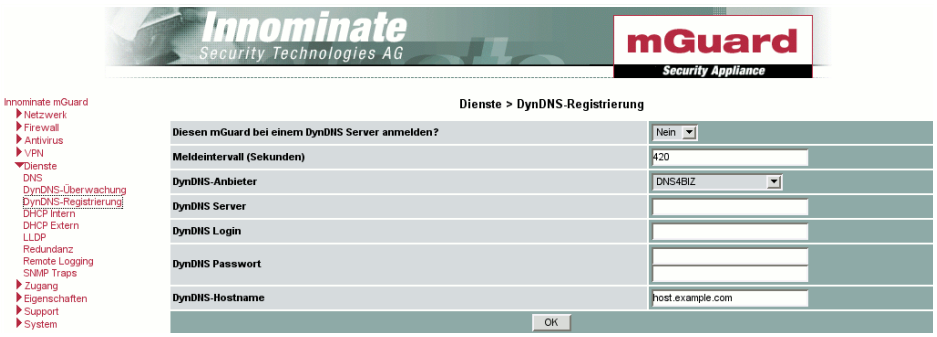


Erläuterung zu DynDNS siehe unten: Dienste → DynDNS Registrierung.

Hostnamen von VPN Gegenstellen überwachen? Ja / Nein
Ist dem mGuard die Adresse einer VPN-Gegenstelle als Hostname angegeben (siehe „VPN → Verbindungen“ auf Seite 49), und ist dieser Hostname bei einem DynDNS Service registriert, dann kann der mGuard regelmäßig überprüfen, ob beim betreffenden DynDNS eine Änderung erfolgt ist. Falls ja, wird die VPN-Verbindung zu der neuen IP-Adresse aufgebaut.

Abfrageintervall (Sekunden)
Standard: 300 (Sekunden)

Dienste → DynDNS Registrierung



Zum Aufbau von VPN-Verbindungen muss mindestens die IP-Adresse eines der Partner bekannt sein, damit diese miteinander Kontakt aufnehmen können. Diese Bedingung ist nicht erfüllt, wenn beide Teilnehmer ihre IP-Adressen dynamisch von ihrem Internet Service Provider zugewiesen bekommen. In diesem Fall kann aber ein DynDNS-Service wie z. B. DynDNS.org oder DNS4BIZ.com helfen. Bei einem DynDNS-Service wird die jeweils gültige IP-Adresse unter einem festen Namen registriert.

Sofern Sie für einen vom mGuard unterstützten DynDNS-Service registriert sind, können Sie in diesem Dialogfeld die entsprechenden Angaben machen.

Diesen mGuard bei einem DynDNS Server anmelden? Ja / Nein

Wählen Sie **Ja**, wenn Sie beim DynDNS-Anbieter entsprechend registriert sind und der mGuard den Service benutzen soll. Dann meldet der mGuard die aktuelle IP-Adresse, die dem eigenen Internet-Anschluss vom Internet Service Provider zugewiesen ist, an den DynDNS Service.

Meldeintervall (Sekunden)

Standard: 420 (Sekunden).

Immer wenn sich die IP-Adresse des eigenen Internet-Anschlusses ändert, informiert der mGuard den DynDNS Service über die neue IP-Adresse. Aus Zuverlässigkeitsgründen erfolgt diese Meldung zusätzlich in dem hier festgelegten Zeitintervall.

Bei einigen DynDNS Anbietern wie z.B. DynDNS.org hat diese Einstellung keine Wirkung, da dort ein zu häufiges Melden zur Löschung des Accounts führen kann.

DynDNS Anbieter

Die zur Auswahl gestellten Anbieter unterstützen das Protokoll, das auch der mGuard unterstützt.

Wählen Sie den Namen des Anbieters aus, bei dem Sie registriert sind, z. B. DynDNS.org

DynDNS Server

Name des Servers des oben ausgewählten DynDNS-Anbieters, z. B.: dyndns.org

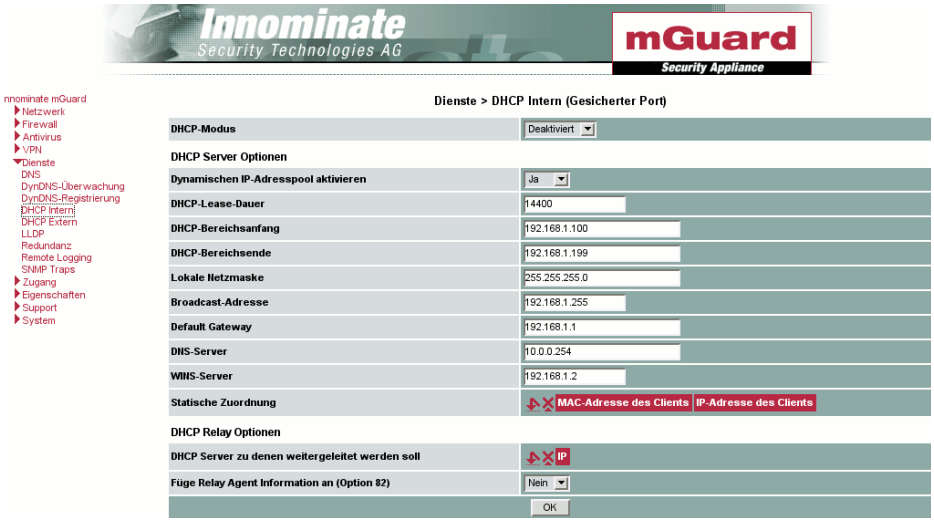
DynDNS Login, DynDNS Passwort

Geben Sie hier den Benutzernamen und das Passwort ein, das Ihnen vom DynDNS-Anbieter zugeteilt worden ist.

DynDNS Hostname

Der für diesen mGuard gewählte Hostname beim DynDNS-Service - sofern Sie einen DynDNS-Dienst benutzen und oben die entsprechenden Angaben gemacht haben.

Dienste → DHCP Intern/Extern



Mit dem Dynamic Host Configuration Protocol (DHCP) kann direkt am mGuard angeschlossenen Clients automatisch die hier eingestellte Netzwerkkonfiguration zugeteilt werden. Unter *DHCP Intern* können Sie DHCP Einstellungen für das interne Interface (LAN) vornehmen und unter *DHCP Extern* die DHCP Einstellungen für das externe Interface (WAN).

DHCP Modus

Setzen Sie diesen Schalter auf **Server**, wenn der mGuard als eigenständiger DHCP Server arbeiten soll.

Setzen Sie ihn auf **Relay**, wenn der mGuard DHCP Anfragen an einen anderen DHCP Server weiterleiten soll.

Steht der Schalter auf **Deaktiviert**, beantwortet der mGuard keine DHCP Anfragen.

⌧ Der DHCP Server/Relay funktioniert auch im Stealth Modus.

DHCP Server Optionen

DHCP-Lease-Dauer

Zeit in Sekunden, für die eine dem Client zugeteilte Netzwerkkonfiguration gültig ist. Kurz vor Ablauf dieser Zeit sollte ein Client seinen Anspruch auf die ihm zugeteilte Konfiguration erneuern. Ansonsten wird diese anderen Rechnern zugeteilt.

Dynamischen IP-Adresspool aktivieren

Setzen Sie diesen Schalter auf **Ja**, wenn sie den durch DHCP-Bereichsanfang bzw. DHCP-Bereichsende gewählten IP-Adresspool verwenden wollen.

Setzen Sie diesen Schalter auf **Nein**, wenn nur statische Zuweisungen anhand der MAC-Adresse vorgenommen werden sollen (siehe unten).

Optionen:

Bei aktiviertem DHCP-Server und aktiviertem dynamischem IP-Adresspool können Sie die Netzwerkparameter angeben, die vom Client benutzt werden sollen:

DHCP-Bereichsanfang: **DHCP-Bereichsende:**	Anfang und Ende des Adressbereichs, aus dem der DHCP-Server des mGuard den lokal angeschlossenen Clients IP-Adressen-zuweisen soll.

Lokale Netzmaske:	Legt die Netzmaske die Clients fest. Voreingestellt ist: 255.255.255.0
Broadcast IP:	Legt die Broadcast IP des Clients fest.
Default-Gateway:	Legt fest, welche IP-Adresse beim Client als Defaultgateway benutzt wird. In der Regel ist das die lokale IP-Adresse des mGuard.
DNS-Server:	Legt fest, wo Clients über den Domain Name Service (DNS) Hostnamen in IP-Adressen auflösen lassen können. Wenn der DNS-Dienst des mGuard genutzt werden soll, dessen lokale IP-Adresse.
WINS-Server:	Legt fest, wo Clients über den Windows Internet Naming Service (WINS) Hostnamen in Adressen auflöst.

Statische Zuordnung [anhand der MAC-Adresse]

Die MAC-Adresse Ihres Clients finden Sie wie folgt heraus:
Windows 95/98/ME: Starten Sie **winipcfg** in einer DOS-Box Windows **NT/2000/XP**: Starten Sie **ipconfig /all** in einer Eingabeaufforderung. Die MAC-Adresse wird als „Physikalische Adresse“ angezeigt.
Linux: Rufen Sie in einer Shell **/sbin/ifconfig** oder **ip link show** auf .

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Bei den Angaben haben Sie folgende Möglichkeiten:

MAC-Adresse des Clients
Die MAC-Adresse (ohne Leerzeichen oder Bindestriche) des Clients.

IP-Adresse des Clients
Die statische IP des Clients, die der MAC-Adresse zugewiesen werden soll.

☞ Die statischen Zuweisungen haben Vorrang vor dem dynamischen IP-Adresspool.
☞ Statische Zuweisungen dürfen sich nicht mit dem dynamischen IP-Adresspool überlappen.
☞ Eine IP darf nicht in mehreren statischen Zuweisungen verwendet werden, ansonsten wird diese IP mehreren MAC-Adressen zugeordnet.
☞ Es sollte nur ein DHCP-Server pro Subnetz verwendet werden.

DHCP Relay Optionen

DHCP Server, zu denen weitergeleitet werden soll
Eine Liste von ein oder mehreren DHCP Servern, an welche DHCP Anfragen weitergeleitet werden sollen.

Füge Relay Agent Information an

Beim Weiterleiten können zusätzliche Informationen nach RFC 3046 für die DHCP Server angefügt werden, an welche weitergeleitet wird.

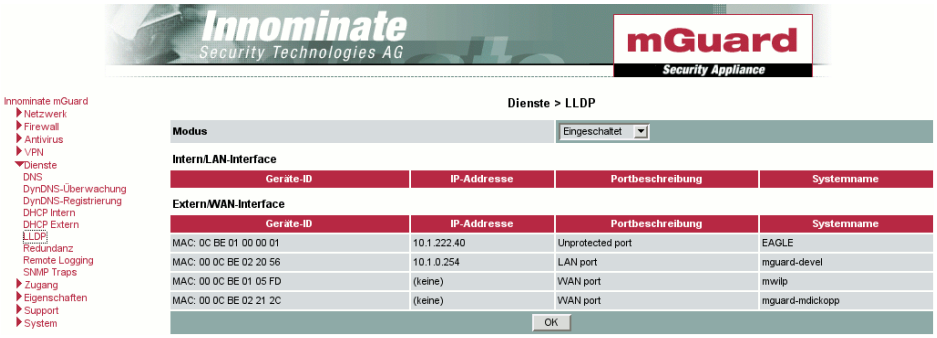
⌦ IP-Konfiguration bei Windows-Clients

Wenn Sie den DHCP-Server des mGuard starten, können Sie die lokal angeschlossenen Clients so konfigurieren, dass sie ihre IP-Adressen automatisch beziehen.

Dazu klicken Sie unter Windows XP **Start, Systemsteuerung, Netzwerkverbindungen**: Symbol des LAN-Adapters mit der rechten Maustaste klikken und im Kontextmenü **Eigenschaften** klicken. Im Dialogfeld *Eigenschatten von LAN-Verbindung* lokales Netz auf der Registerkarte *Allgemein* unter „Diese Verbindung verwendet folgende Elemente“ den Eintrag **Internetprotokoll (TCP/IP)** markieren und dann die Schaltfläche **Eigenschaften** klicken.

Im Dialogfeld *Eigenschaften von Internetprotokoll (TCP/IP)* die gebotenen Angaben bzw. Einstellungen machen.

Dienste → LLDP



Mit LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) kann mit geeigneten Abfragemethoden die (Ethernet) Netzwerk-Infrastruktur automatisch ermittelt werden. Auf Ethernet-Ebene (Layer 2) werden dazu periodisch Multicasts versandt, aus denen dann Tabellen der ans Netz angeschlossener Systeme erstellt werden, die über SNMP abgefragt werden können.

Modus

Der LLDP-Service bzw. -Agent kann hier global ein- bzw. ausgeschaltet werden.

Internes/LAN-Interface und Externes/WAN-Interface

Geräte-ID

Eine eindeutige ID des gefundenen Rechners; üblicherweise eine seiner MAC-Adressen.

IP-Adresse

IP-Adresse des gefundenen Rechners über welcher er per SNMP administriert werden kann.

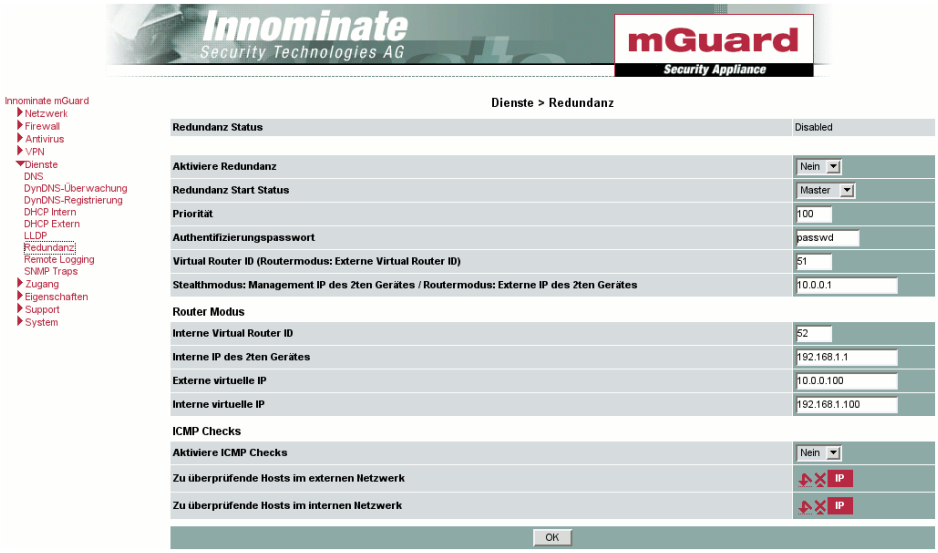
Portbeschreibung

Ein Text, welcher die Netzwerkschnittstelle beschreibt, über welche der Rechner gefunden wurde.

Systemname

Hostname des gefundenen Rechners.

Dienste → Redundanz (nur mGuard enterprise XL)



Mit Hilfe der Redunzanzfähigkeit ist es möglich, zwei mGuards zu einem virtuellen Router zusammenzufassen. Ein zweiter mGuard (Backup) übernimmt dabei in einem Fehlerfall die Funktion des ersten mGuards (Master).
Weiterhin wird der Zustand der Statefull Firewall zwischen beiden mGuards fortwährend synchronisiert, so dass bei einem Wechsel bestehende Verbindungen nicht abgebrochen werden.

- Voraussetzung: Beide mGuards müssen entsprechend konfiguriert werden. Die Firewalleinstellungen sollten identisch sein, damit nach der Umschaltung keine Probleme auftreten.
- Redundanz wird im Router Modus, im statischen Stealth Modus mit Management IP und im multi Stealth Modus unterstützt.
- Bei aktivierter Redundanz dürfen die beiden mGuards nicht als VPN-Gateway genutzt werden.
- Die interne virtuelle IP muß bei Geräten, die mit dem internen Netzwerk der mGuards verbunden sind, als Default Gateway konfiguriert werden.

Die folgenden Funktionen/Dienste können bei aktivierter Redundanz genutzt werden:

- Eingehende/ausgehende Firewall Regeln
- NAT (IP-Masquerading, d.h. ausgehender Netzwerkverkehr wird auf die externe virtuelle IP umgeschrieben.)
- 1:1 NAT
- Port Weiterleitung (für *Eingehend auf IP* muß die externe virtuelle IP konfiguriert werden)
- MAC-Filter

Aktiviere Redundanz

Redundanz aktivieren/deaktivieren.

Redundanz Start Status

Status des mGuards bei Aktivierung der Redundanz (Master oder Backup).

Priorität

Entscheidet, welcher mGuard als Master fungiert.

Sind die Prioriäten unterschiedlich gesetzt, so arbeitet der mGuard mit der höheren Priorität als Master solange er nicht ausfällt.

Haben beide mGuards die gleiche Priorität und wird im Fehlerfall der Backup zum Master, so arbeitet dieser auch dann als Master weiter, wenn der vorherige mGuard wieder zur Verfügung steht.

Werte zwischen 1 und 254 sind möglich.

Authentifizierungspasswort

Das Passwort soll vor Fehlkonfigurationen schützen, bei denen sich mehrere virtuelle Router gegenseitig stören.

Das Passwort muss auf beiden mGuards gleich sein. Es wird im Klartext übermittelt und sollte daher nicht identisch mit anderen sicherheitsrelevanten Passwörtern sein.

Virtual Router ID (Routermodus: Externe Virtual Router ID)

Eine ID zwischen 1 und 255, die auf beiden mGuards gleich sein muss und den virtuellen Router identifiziert.

Management IP des 2ten Gerätes (Routermodus: Externe IP des 2ten Gerätes)

Im Stealthmodus die Management IP des zweiten mGuards, im Routermodus die externe IP des zweiten mGuards.

Router Modus

Die folgenden Werte müssen gesetzt werden, wenn die mGuards im Router Modus betrieben werden.

Interne Virtual Router ID

Eine ID zwischen 1 und 255, die auf beiden mGuards gleich sein muss und den virtuellen Router am internen Interface identifiziert.

Interne IP des 2ten Gerätes

Die interne IP des zweiten mGuards.

Externe virtuelle IP

Virtuelle IP, über die der Verkehr durch den mGuard läuft. Wird z.B. bei NAT als externe IP verwendet.

Interne virtuelle IP

Virtuelle IP, über die der Verkehr durch den mGuard läuft. Muss z.B. als Defaultgateway auf den Clients im internen Netzwerk eingestellt werden.

ICMP Checks

ICMP Checks bilden eine zusätzliche Möglichkeit der Überwachung der Netzwerkverbindungen zwischen den mGuards, die als virtueller Router zusammenarbeiten.

Fällt nur die interne oder die externe Netzwerkverbindung zwischen Master und Backup aus, so wird der Backup zum Master. Das vom Guard verwendete Virtual Router Redundancy Protocol (VRRP) kann den noch funktionierenden Master jedoch nicht darüber informieren. Über die noch funktionierenden Netzwerkverbindung würden die zwei Master anschließend miteinander in Konflikt stehen.

Über die ICMP Checks (ICMP Ping) kann der Master daher die Verbindung zum Backup überprüfen und sich gegebenenfalls deaktivieren.

Aktiviere ICMP Checks

Überwache die Verbindung zum Backup mit Hilfe des ICMP Protokolls.

Ist der Backup mGuard nicht mehr zu erreichen, versucht der Master nacheinander die unter *Zu überprüfende Hosts im externen/internen Netzwerk* angegebenen Hosts zu erreichen.

Sind auch diese nicht erreichbar, deaktiviert sich der Master.

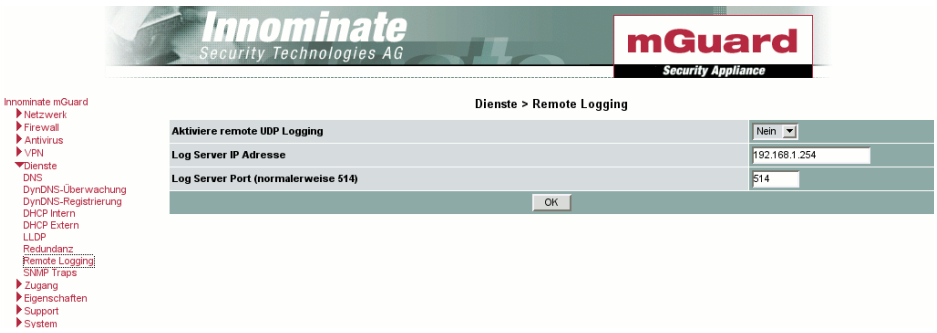
Zu überprüfende Hosts im externen Netzwerk

Zu überprüfende Hosts im externen Netzwerk. Diese müssen ICMP Echo Requests beantworten können.

Zu überprüfende Hosts im internen Netzwerk

Zu überprüfende Hosts im internen Netzwerk. Diese müssen ICMP Echo Requests beantworten können.

Dienste → Remote Logging



Alle Log-Einträge finden standardmäßig im Arbeitsspeicher des mGuard statt. Ist der maximale Speicherplatz für diese Protokollierungen erschöpft, werden automatisch die ältesten Log-Einträge durch neue überschrieben. Zudem werden bei Ausschalten des mGuard alle Log-Einträge gelöscht.

Um das zu verhindern, ist es möglich, die Log-Einträge auf einen externen Rechner zu übertragen. Das liegt auch dann nahe, sollte eine zentrale Verwaltung der Protokollierungen erfolgen.

Aktiviere remote UDP Logging: Ja / Nein

Sollen alle Log-Einträge zum externen (unten angegebenen) Log Server übertragen werden, setzen Sie diesen Schalter auf **Ja**.

Log Server IP Adresse

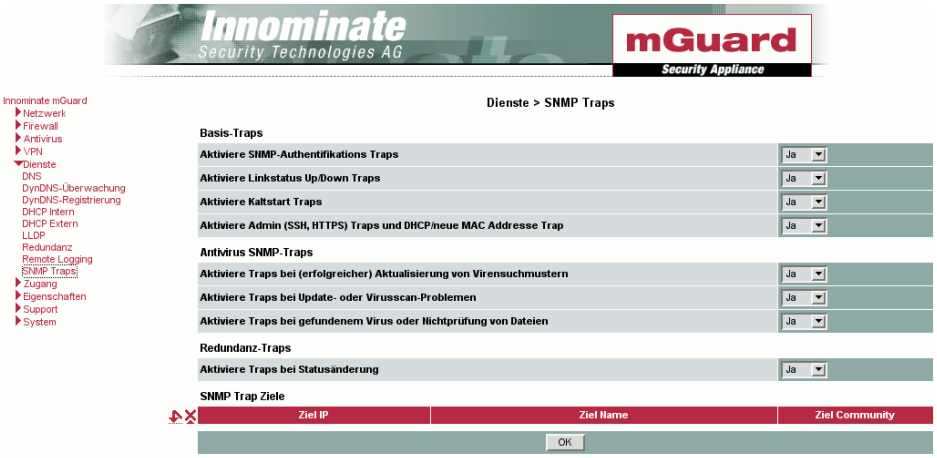
Geben Sie die IP-Adresse des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen.

☞ Sie müssen eine IP-Adresse angeben, keinen Hostnamen! Hier wird eine Namensauflösung nicht unterstützt, weil sonst der Ausfall eines DNS-Servers nicht protokolliert werden könnte.

Log Server Port

Geben Sie den Port des Log Servers an, zu dem die Log-Einträge per UDP übertragen werden sollen. Standard: 514

Dienste → SNMP Traps



Bei bestimmten Ereignissen kann der mGuard SNMP Traps versenden. Die folgenden Einstellungen sind möglich:

- **Basis-Traps**Aktiviere SNMP-Authentifikations Traps
- Aktiviere Linkstatus Up/Down Traps
- Aktiviere Kaltstart Traps
- Aktiviere Admin (SSH, HTTPS) Traps und DHCP/neue MAC Addresse Trap

Antivirus SNMP-Traps

- Aktiviere Traps bei (erfolgreicher) Aktualisierung von Virensuchmustern
- Aktiviere Traps bei Update- oder Virusscan-Problemen
- Aktiviere Traps bei gefundenem Virus oder Nichtprüfung von Dateien

Redundanz Traps

- Aktiviere Traps bei Statusänderung.

SNMP Trap Ziele

Traps können an mehrere Ziele versendet werden.

Ziel IP

IP, an welche der Trap gesendet werden soll.

Ziel Name

Ein optionaler beschreibender Name für das Ziel, welcher keinen Einfluß auf die generierten Traps hat.

Ziel Community

Name der SNMP-Community, welcher der Trap zugeordnet ist.

5.11 Menü Zugang

Zugang → Passworte

Der mGuard bietet 3 Stufen von Benutzerrechten. Um sich auf der entsprechenden Stufe anzumelden, muss der Benutzer das Passwort angeben, das der jeweiligen Berechtigungsstufe zugeordnet ist.

Berechtigungsstufe	
Root	Bietet vollständige Rechte für alle Parameter des mGuard. Hintergrund: Nur diese Berechtigungsstufe erlaubt es, sich per SSH so mit dem Gerät zu verbinden, dass man das ganze System auf den Kopf stellen kann. Dann kann man es nur noch mit „Flashen“ der Firmware in seinen Auslieferungszustand zurückbringen (siehe „Flashen der Firmware“ auf Seite 91). Voreingestelltes Rootpasswort: **root**
Administrator	Bietet die Rechte für die Konfigurationsoptionen, die über die webbasierte Administratoroberfläche zugänglich sind. Voreingestellter Benutzername: **admin** Voreingestelltes Passwort: **mGuard** Der Benutzername **admin** kann nicht geändert werden.
Nutzer	Ist ein Nutzerpasswort festgelegt und aktiviert, dann muss der Benutzer nach jedem Neustart des mGuard bei Zugriff auf eine beliebige HTTP URL dieses Passwort angeben, damit VPN-Verbindungen möglich sind. Wollen Sie diese Option nutzen, legen Sie im entsprechenden Eingabefeld das Nutzerpasswort fest.

Rootpasswort

Werksseitig voreingestellt: **root**

Wollen Sie das Rootpasswort ändern, geben Sie ins Feld *Altes Passwort* das alte Passwort ein, in die beiden Felder darunter das neue gewünschte Passwort.

Administratorpasswort (Account: admin)

Werksseitig voreingestellt: **mGuard** (unveränderbarer Benutzername: admin)

Aktiviere Nutzerpasswort: Nein / Ja

Werksseitig ist Nutzer-Passwortschutz ausgeschaltet.

Ist unten ein Nutzerpasswort festgelegt, kann der Nutzer-Passwortschutz mit diesem Schalter aktiviert bzw. deaktiviert werden.

Nutzerpasswort

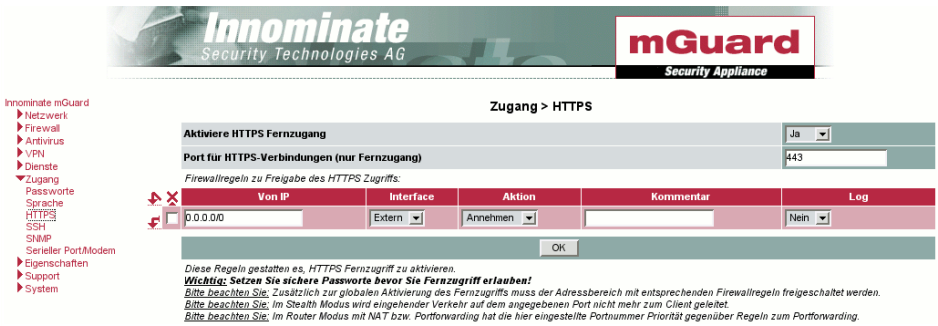
Werkseitig ist kein Nutzerpasswort voreingestellt. Um eines festzulegen, geben Sie in beide Eingabefelder übereinstimmend das gewünschte Passwort ein.

Zugang → Sprache

Bitte wählen Sie eine Sprache aus

Ist in der Sprachauswahlliste **(Automatisch)** ausgewählt, übernimmt das Gerät die Spracheinstellung aus dem Browser des Rechners.

Zugang → HTTPS



Bei eingeschaltetem HTTPS Fernzugang kann der mGuard über seine webbasierte Administratoroberfläche von einem entfernten Rechner aus konfiguriert werden. Das heißt, auf dem entfernten Rechner wird der Browser benutzt, um den lokalen mGuard zu konfigurieren.
Standardmäßig ist diese Option ausgeschaltet.

WICHTIG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass ein sicheres Root- und Administrator-Passwort festgelegt ist.

Um HTTPS Fernzugang zu ermöglichen, machen Sie nachfolgende Einstellungen:

Aktiviere HTTPS Fernzugang: Ja / Nein

Wollen Sie HTTPS Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**.

☞ Achten Sie in diesem Fall darauf, die auf dieser Seite befindlichen Firewall-Regeln so zu setzen, dass von außen auf den mGuard zugegriffen werden kann.

Port für HTTPS-Verbindungen (nur Fernzugang)

Standard: 443

Sie können einen anderen Port festlegen.

Die entfernte Gegenstelle, die den Fernzugriff ausübt, muss bei der Adressenangabe hinter die IP-Adresse die Port-Nummer angeben, die hier festgelegt ist.

Beispiel:

Ist dieser mGuard über die Adresse 123.456.789.21 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 443 festgelegt, dann muss bei der entfernten Gegenstelle im Web-Browser diese Port-Nummer nicht hinter der Adresse angegeben werden.

Bei einer anderen Port-Nummer ist diese hinter der IP-Adresse anzugeben, z. B. wie folgt: https://123.456.7890.21:442/

Firewall-Regeln zur Freigabe des HTTPS-Zugriffs

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines HTTP-Fernzugriffs.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89

Interface

extern (fest vorgegeben).

Aktion

Möglichkeiten:

- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen* - s. u.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

☞ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Zugang → SSH

Bei eingeschaltetem SSH Fernzugang kann der mGuard von einem entfernten Rechner aus über die Kommandozeile konfiguriert werden.
Standardmäßig ist diese Option ausgeschaltet.

WICHTIG: Wenn Sie Fernzugriff ermöglichen, achten Sie darauf, dass ein sicheres Root- und Administrator-Passwort festgelegt ist.

Um SSH Fernzugang zu ermöglichen, machen Sie folgende Einstellungen:

Aktiviere SSH Fernzugang: Ja / Nein

Wollen Sie SSH Fernzugriff ermöglichen, setzen Sie diesen Schalter auf **Ja**.

☞ Achten Sie in diesem Fall darauf, die auf dieser Seite befindlichen Firewall-Regeln so zu setzen, dass von außen auf den mGuard zugegriffen werden kann.

Port für SSH-Verbindungen (nur Fernzugang)

Standard: 22

Sie können einen anderen Port festlegen.

Beispiel:

Ist dieser mGuard über die Adresse 123.456.789.21 über das Internet zu erreichen, und ist für den Fernzugang die Port-Nummer 22 festgelegt, dann muss bei der entfernten Gegenstelle im SSH-Client (z. B. PuTTY oder OpenSSH) diese Port-Nummer evtl. nicht angegeben werden.

Bei einer anderen Port-Nummer (z. B. 22222) ist diese anzugeben, z. B.:
ssh -p 22222 123.456.789.21

Firewall-Regeln zur Freigabe des SSH-Zugriffs

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SSH-Fernzugriffs.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- IP-Adresse: **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89

Interface

extern (fest vorgegeben).

Aktion

Möglichkeiten:

- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

☞ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

Kommentar

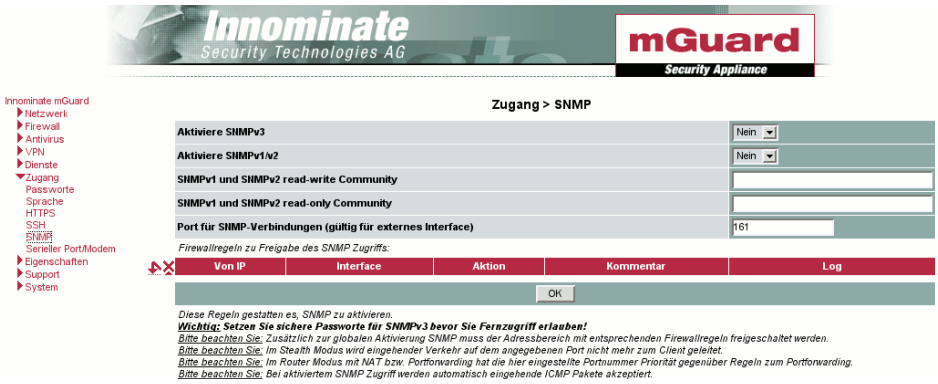
Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Zugang → SNMP



Das SNMP (Simple Network Management Protokoll) wird vorzugsweise in komplexeren Netzwerken benutzt, um den Zustand und den Betrieb von Geräten zu überwachen.

Das SNMP gibt es in mehreren Entwicklungsstufen: SNMPv1/SNMPv2 und SNMPv3.

Die älteren Versionen SNMPv1/SNMPv2 benutzen keine Verschlüsselung und gelten als nicht sicher. Daher ist davon abzuraten, SNMPv1/SNMPv2 zu benutzen.

SNMPv3 ist unter dem Sicherheitsaspekt deutlich besser, wird aber noch nicht von allen Management-Konsolen unterstützt.

⌧ SNMP-„Get“- oder „Walk“-Anfragen können länger als eine Sekunde dauern. Dieser Wert entspricht jedoch dem Standard-Timeout-Wert einiger SNMP-Management-Applikationen.

Bitte setzen Sie aus diesem Grund den Timeout-Wert Ihrer Management Applikation auf Werte zwischen 3 und 5 Sekunden, falls Timeout-Probleme auftreten sollten.

Aktiviere SNMPv3: Ja / Nein

Wollen Sie zulassen, dass der mGuard per SNMPv3 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**.

Für den Zugang per SNMPv3 ist eine Authentifizierung mittels Login und Paßwort notwendig. Die Werkseinstellungen für die Login-Parameter lauten:

Login: admin

Passwort: SnmpAdmin

Für die Authentifizierung wird MD5 unterstützt, für die Verschlüsselung DES.

Die Login-Parameter für SNMPv3 können nur mittels SNMPv3 geändert werden.

Aktiviere SNMPv1/v2: Ja / Nein

Wollen Sie zulassen, dass der mGuard per SNMPv1/v2 überwacht werden kann, setzen Sie diesen Schalter auf **Ja**.

Zusätzlich müssen Sie die nachfolgenden Login-Daten angeben:

SNMPv1 und SNMPv2 read-write Community

SNMPv1 und SNMPv2 read-only Community

Geben Sie in diese Felder die erforderlichen Login-Daten ein.

Port für SNMP-Verbindungen (gültig für externes Interface)

Standard: 161

Firewall-Regeln zur Freigabe des SNMP-Zugriffs

Listet die eingerichteten Firewall-Regeln auf. Sie gelten für eingehende Datenpakete eines SNMP-Zugriffs.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Von IP

Geben Sie hier die Adresse des Rechners oder Netzes an, von dem der Fernzugang erlaubt ist.

Bei den Angaben haben Sie folgende Möglichkeiten:

- Von IP
- **0.0.0.0/0** bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless Inter-Domain Routing)“ auf Seite 89.

Interface

extern (fest vorgegeben).

Aktion

Möglichkeiten:

- Annehmen
- Abweisen
- Verwerfen

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält. (Im *Stealth*-Modus hat *Abweisen* dieselbe Wirkung wie *Verwerfen*.)

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

☞ Im Stealth-Modus ist *Abweisen* als Aktion nicht möglich.

Kommentar

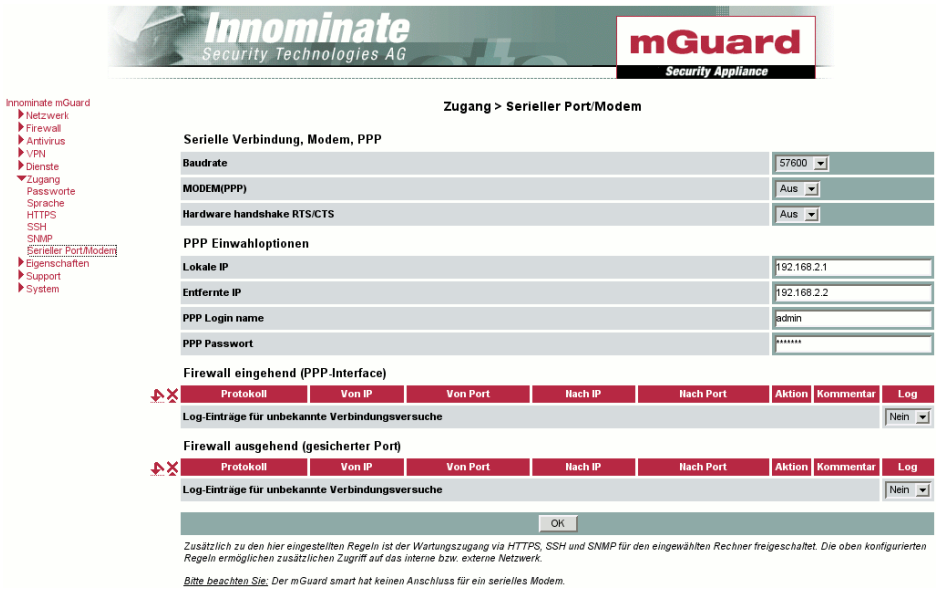
Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- oder das Ereignis nicht protokolliert werden soll - *Log* auf **Nein** setzen (werkseitige Voreinstellung).

Zugang → Serieller Port/Modem



Einige mGuards wie der mGuard blade oder industrial verfügen über eine von außen zugängliche serielle Schnittstelle. Über diese kann man mittels eines Terminalprogramms oder aber einer PPP Verbindung auf den mGuard zugreifen.

Serielle Verbindung, Modem, PPP

Baudrate
Die zu verwendende Geschwindigkeit auf dem seriellen Port

MODEM(PPP)
Wenn diese Option auf **Aus** steht, kann man sich über ein Terminal über den seriellen Port einloggen. Steht sie auf **Ein**, kann man sich über PPP auf dem mGuard einloggen.

Hardware handshake RTS/CTS
Nutze die RTS und CTS Signale für die PPP Verbindung.

PPP Einwahloptionen

Lokale IP
IP des mGuard für die PPP Verbindung.

Entfernte IP
IP der Gegenstelle für die PPP Verbindung.

PPP Login name
Login, welchen die PPP Gegenstelle angeben muß um die PPP Verbindung aufbauen zu können.

PPP Passwort
Das Passwort, welches die Gegenstelle angeben muß.

Firewall eingehend (PPP-Interface)

Firewallregeln für Verbindungen von PPP zum lokalen Ethernetinterface (LAN).

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Bei den Angaben haben Sie folgende Möglichkeiten:

Protokoll
Alle bedeutet: TCP, UDP, ICMP und andere IP-Protokolle.

IP-Adresse

0.0.0.0/0 bedeutet alle Adressen. Um einen Bereich anzugeben, benutzen Sie die CIDR-Schreibweise - siehe „CIDR (Classless InterDomain Routing)“ auf Seite 89.

Port

(wird nur ausgewertet bei den Protokollen TCP und UDP)

any bezeichnet jeden beliebigen Port.

startport:endport (z. B. 110:120) bezeichnet einen Portbereich.

Einzelne Ports können Sie entweder mit der Port-Nummer oder mit dem entsprechenden Servicenamen angegeben: (z. B. 110 für pop3 oder pop3 für 110).

Aktion

Annehmen bedeutet, die Datenpakete dürfen passieren.

Abweisen bedeutet, die Datenpakete werden zurückgewiesen, so dass der Absender eine Information über die Zurückweisung erhält.

Verwerfen bedeutet, die Datenpakete dürfen nicht passieren. Sie werden verschluckt, so dass der Absender keine Information erhält über deren Verbleib.

Kommentar

Ein frei wählbarer Kommentar für diese Regel.

Log

Für jede einzelne Firewall-Regel können Sie festlegen, ob bei Greifen der Regel

- ☞ das Ereignis protokolliert werden soll - *Log* auf **Ja** setzen
- ☞ oder nicht - *Log* auf **Nein** setzen (werksseitige Voreinstellung).

Log-Einträge für unbekannte Verbindungsversuche

Damit werden alle Verbindungsversuche protokolliert, die nicht von den voranstehenden Regeln erfasst werden.

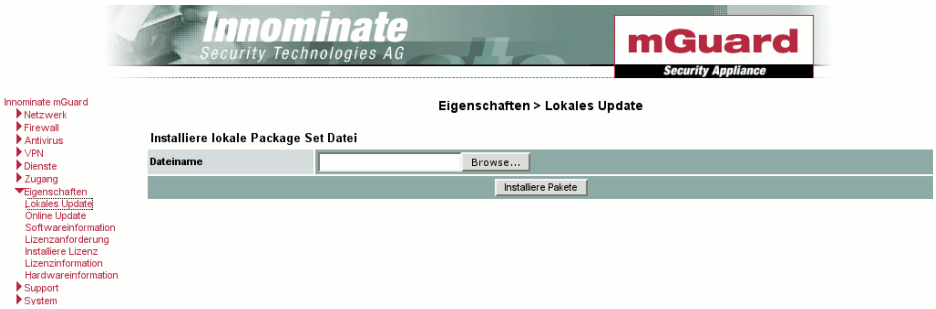
Firewall ausgehend (gesicherter Port)

Firewallregeln für Verbindungen vom lokalen Ethernetinterface (LAN) nach PPP.

(Alle weiteren Angaben entsprechen *Firewall eingehend (ungesicherter Port)*.)

5.12 Menü Eigenschaften

Eigenschaften → Lokales Update



Lesen Sie die README-Datei!

Voraussetzung: Sie haben ein aktuelles Software-Paket lokal auf Ihrem Konfigurations-Rechner gespeichert.

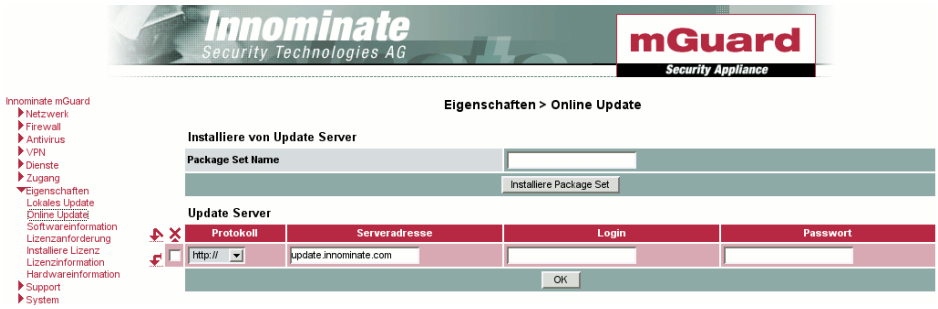
- Ob und auf welche Weise Sie an ein Software-Update gelangen können, erfragen Sie bei Ihrem Distributor.
- **Sie dürfen während des Updates auf keinen Fall die Stromversorgung des mGuard unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.**

Haben Sie ein aktuelles Software-Update auf Ihrem Konfigurations-Rechner gespeichert, gehen Sie wie folgt vor:

1. **Durchsuchen...** klicken und dann die Datei selektieren.
2. **Installiere Pakete** klicken, um sie in das Gerät zu laden.
   Dieser Vorgang kann je nach Größe des Updates mehrere Minuten dauern.

Sollte nach dem System-Update ein Reboot erforderlich sein, wird das angezeigt.

Eigenschaften → Online Update



Voraussetzung: Sie haben ein aktuelles Software-Paket über einen entfernten Server zur Verfügung gestellt bekommen.

- Ob und auf welche Weise Sie an ein Software-Update gelangen können, erfragen Sie bei Ihrem Distributor.
- **Sie dürfen während des Updates auf keinen Fall die Stromversorgung des mGuard unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.**

Gehen Sie wie folgt vor:

1. Schreiben Sie den Dateinamen in das Feld **Package Set Name**.
2. **Installiere Package Set** klicken, um sie in das Gerät zu laden.
   Dieser Vorgang kann je nach Größe des Updates mehrere Minuten dauern.

Sollte nach dem System-Update ein Reboot erforderlich sein, wird das angezeigt.

Update Server

Geben Sie hier die Server an, von denen sich der mGuard seine Updates holen

soll.

Protokoll

Die Updatedateien kann entweder per HTTP oder HTTPS auf den mGuard geladen werden.

Serveradresse

FQDN oder IP-Adresse des Servers, auf dem sich die Updatedateien befinden, z.B. „123.456.789.21“ oder „update.example.com“.

Login

Login für den Server.

Passwort

Passwort für den Login.

☞ Das Einfügen, Verschieben und Löschen von Zeilen ist unter „Arbeiten mit Tabellen“ auf Seite 15 beschrieben.

Eigenschaften → Installiere Lizenz

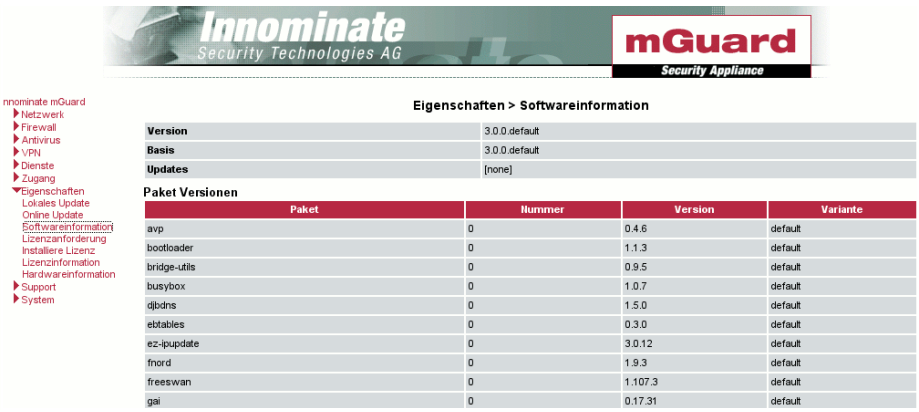
Voraussetzung: Sie haben von Ihrem Distributor eine Lizenzdatei für den mGuard erworben und haben diese Datei auf dem Konfigurations-Rechner gespeichert.

Installieren Sie die Lizenzdatei wie folgt:

1. **Durchsuchen...** klicken und dann die Datei selektieren.
2. **Installiere Lizenzdatei** klicken, um sie in das Gerät zu laden.

Features → Software-information

Nur Anzeige



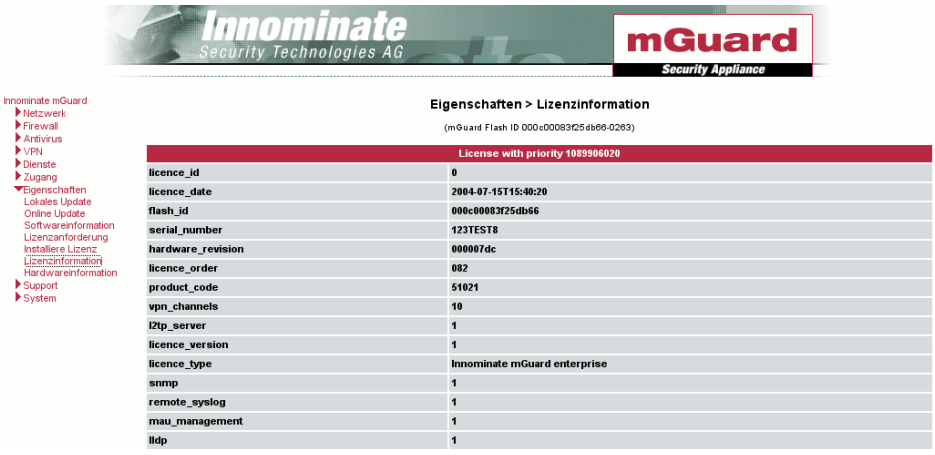
Listet die im Gerät befindlichen Software-Module auf. Diese werden als Pakete bezeichnet.

Dient für Update-Zwecke: Vergleichen Sie die angezeigten Versionsnummern mit den aktuellen Versionsnummern der entsprechenden Pakete. Bitte wenden Sie sich dazu an Ihren Distributor.

Falls neue Versionen verfügbar sind, können Sie die Software im Gerät updaten. Siehe „Eigenschaften → Lokales Update“ auf Seite 79.

Eigenschaften → Lizenzinformation

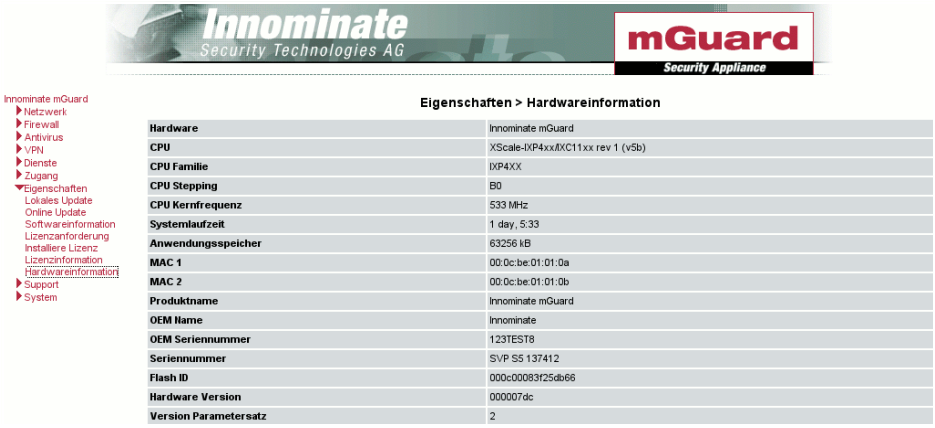
Nur Anzeige



Listet die erworbenen Lizenzen auf. Die entsprechenden Lizenzdateien sind im mGuard installiert. Siehe „Eigenschaften → Installiere Lizenz“ auf Seite 80.

Eigenschaften → Hardware-information

Nur Anzeige



Für erfahrene Systemadministratoren / Support.

5.13 Menü Support

Support → Snapshot

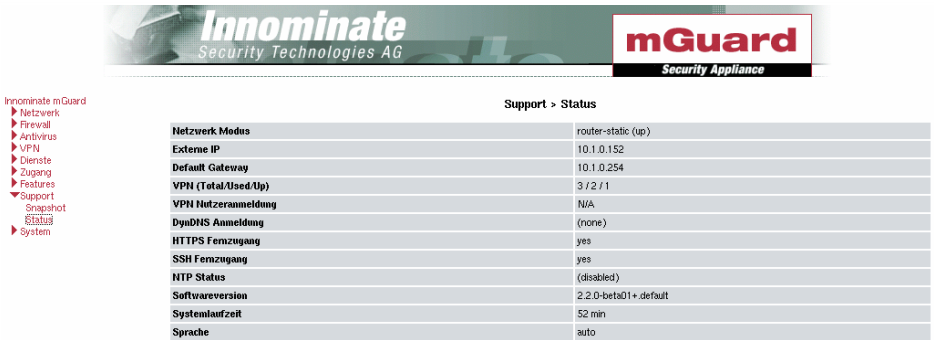
Diese Funktion dient für Support-Zwecke des Innominate Support.
Erstellt eine komprimierte Datei (im tar-Format), in der alle aktuellen Konfigurations-Einstellungen und Log-Einträge erfasst sind, die zur Fehlerdiagnose relevant sein könnten. (Diese Datei enthält keine privaten Informationen wie z. B. das private Maschinen-Zertifikat oder die Passwörter. Eventuell benutzte Pre-Shared Keys von VPN-Verbindungen sind jedoch in den Snapshots enthalten.)
Um einen Snapshot zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie **Herunterladen**.
2. Speichern Sie die Datei unter dem Namen *snapshot.tar.gz*

Stellen Sie die Datei dem Support zur Verfügung, wenn dieser danach fragt.

Support → Status

Nur Anzeige



Zeigt eine Zusammenfassung verschiedener Statusinformationen für Support-Zwecke:

Netzwerk-Modus: Betriebsart des mGuard: *Stealth*, *Router*, *PPPoE* oder *PPTP*

Externe IP: Die IP-Adresse des mGuard an seinem Anschluss für das externe Netz (WAN bzw. Internet).
Im *Stealth*-Modus übernimmt der mGuard die Adresse des lokal angeschlossenen Rechners für diese Schnittstelle.

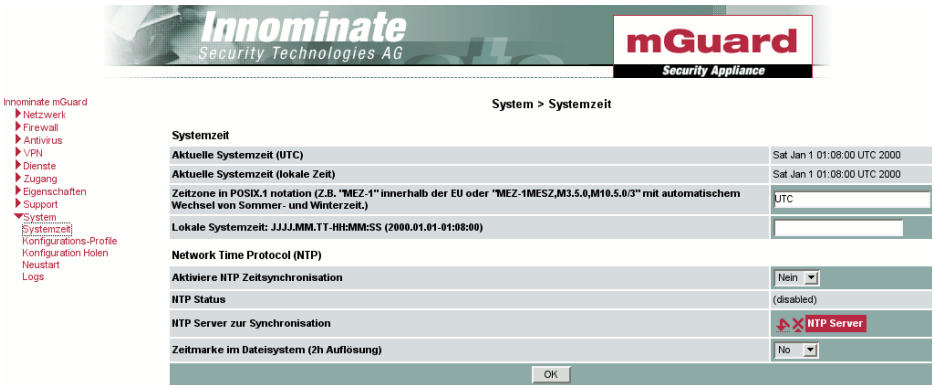
Default Gateway: Hier wird die IP-Adresse angezeigt, über die der mGuard versucht ihm unbekannte Netze zu erreichen.Im *Stealth*-Modus oder falls die in der Konfiguration angegebene IP nicht erreichbar ist steht hier „(none)“.

VPN (Total / Used / Up): Möglichkeiten: *Total* / *Used* / *Up*
Total: Insgesamt eingerichtete VPN-Verbindungen
Used: Benutzte VPN-Verbindungen
Up: Gegenwärtig aktive VPN-Verbindungen

VPN Nutzeranmeldung:	Möglichkeiten: *N / A* : Nicht verfügbar (not available) *not logged in* : VPN gesperrt *logged in* : VPN freigeschaltet
DynDNS Anmeldung:	Möglichkeiten: *none / Angabe des DynDNS-Server / failure / trying* *none*: Kein DynDNS-Server angegeben *Angabe des DynDNS-Server*: Adresse des DynDNS-Servers, den der mGuard zum Registrieren seiner IP benutzt. *failure*: Der mGuard versucht vergeblich, eine Verbindung zum DynDNS-Server herzustellen. *trying*: Der mGuard versucht gerade, eine Verbindung zum DynDNS-Server herzustellen.
HTTPS Fernzugang:	Möglichkeiten: *no / yes*
SSH Fernzugang:	Möglichkeiten: *no / yes*
NTP Status:	Möglichkeiten: *synchonized / not synchronized* *synchronized*: Über das Network Time Protokoll empfängt der mGuard von einem Zeitserver die aktuelle Uhrzeit (Greenwich-Zeit). *not synchronized*: Der mGuard ist mit keinem Zeitserver verbunden und kann deshalb nicht die aktuelle Uhrzeit liefern.
Softwareversion:	Version der im mGuard installierten Software
Systemlaufzeit:	Laufzeit seit dem letzten Startvorgang des mGuard.
Sprache:	Aktuell eingestellte Sprache

5.14 Menü System

Dienste → System-zeit



Systemzeit

Aktuelle Systemzeit (UTC)

Anzeige der aktuellen Systemzeit in Universal Time Coordinates (UTC). Wenn die *NTP Zeitsynchronisation* noch nicht aktiviert ist (s. u.), und *Zeitmarken im Dateisystem* deaktiviert sind, beginnt die Uhr mit dem 1. Januar 2000.

Aktuelle Systemzeit (lokale Zeit)

Soll die eventuell abweichende aktuelle Ortszeit angezeigt werden, müssen Sie unter *Zeitzone in POSIX.1 Notation...* (s. u.) den entsprechenden Eintrag machen.

Zeitzone in POSIX.1 Notation...

Soll oben unter *Aktuelle Systemzeit* nicht die mittlere Greenwich-Zeit angezeigt werden sondern Ihre aktuelle Ortszeit (abweichend von der mittleren Greenwich-Zeit), dann tragen Sie hier ein, um wieviel Stunden bei Ihnen die Zeit voraus bzw. zurück ist.

Beispiele:

In Berlin ist die Uhrzeit der mittleren Greenwich-Zeit um 1 Stunde voraus. Also tragen Sie ein: MEZ-1

Wichtig ist allein die Angabe -1, -2 oder +1 usw., weil nur sie ausgewertet wird; die davor stehenden Buchstaben nicht. Sie können „MEZ“ oder beliebig anders lauten.

Wünschen Sie die Anzeige der MEZ-Uhrzeit (= gültig für Deutschland) mit automatischer Umschaltung auf Sommer- bzw. Winterzeit geben Sie ein: MEZ-1MESZ,M3.5.0,M10.5.0/3

Lokale Systemzeit

Hier können Sie die Zeit des mGuards setzen falls kein NTP Server eingestellt wurde oder aber der NTP Server nicht erreichbar ist.

Das Datum und die Zeit werden in dem Format JJJJ.MM.TT-ss:mm angegeben:

JJJJ	Jahr
MM	Monat
TT	Tag
ss	Stunde
mm	Minute

Network Time Protocol (NTP)

Aktiviere NTP Zeitsynchronisation: Ja / Nein

Sobald das NTP aktiviert ist, bezieht der mGuard die Zeit aus dem Internet und zeigt diese als aktuelle Systemzeit an. Die Synchronisation kann einige Sekunden dauern.

Nur wenn dieser Schalter auf **Ja** steht und unter *NTP Server zur Synchronisation* (s. u.) mindestens 1 Zeitserver angegeben ist, wird die aktuelle Systemzeit über das Internet bezogen.

NTP Status

Anzeige des aktuellen NTP-Status

NTP Server zur Synchronisation

Geben Sie hier einen oder mehrere Zeitserver an, von denen der mGuard die aktuelle Zeitangabe beziehen soll. Falls Sie mehrere Zeitserver angeben, verbindet sich der mGuard automatisch mit allen, um die aktuelle Zeit zu ermitteln.

☞ Wenn Sie statt einer IP-Adresse einen Hostnamen, z. B. pool.ntp.org, angeben, muss ein gültiger DNS-Server festgelegt sein - siehe „Dienste → DNS“ auf Seite 61.

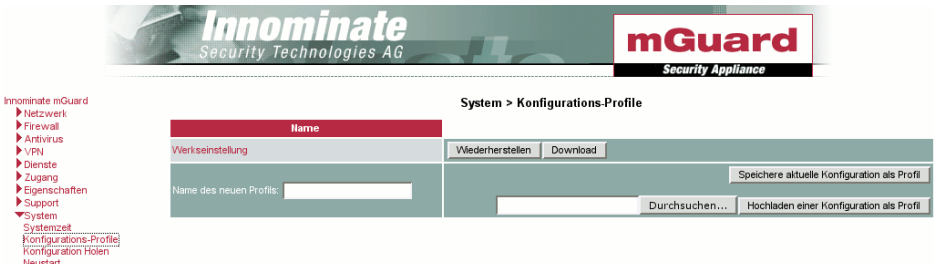
☞ Arbeitet der mGuard im *Router- PPPoE-* oder *PPTP*-Modus, stellt er auch den angeschlossenen Rechnern die NTP-Zeit zur Verfügung.

Zeitmarke im Dateisystem (2h Auflösung): Ja / Nein

Ist dieser Schalter auf **Ja** gesetzt, schreibt der mGuard alle 2 Stunden die aktuelle Systemzeit in seinen Speicher.

Folge: Wird der mGuard aus- und wieder eingeschaltet, wird nach dem Einschalten eine Uhrzeit in diesem 2-Stunden-Zeitfenster angezeigt und nicht eine Uhrzeit am 1. Januar 2000.

System → Konfigurations-profile



Sie haben die Möglichkeit, die Einstellungen des mGuard als Konfigurations-Profil unter einem beliebigen Namen im mGuard zu speichern. Sie können mehrere solcher Konfigurations-Profile anlegen, so dass Sie nach Bedarf zwischen verschiedenen Profilen wechseln können, z.B. wenn der mGuard in unterschiedlichen Umgebungen eingesetzt wird.

Darüber hinaus können Sie Konfigurations-Profile als Dateien auf ihrem Konfigurations-Rechners abspeichern. Umgekehrt besteht die Möglichkeit, eine so erzeugte Konfigurationsdatei in den mGuard zu laden und zu aktivieren.

Zusätzlich haben Sie die Möglichkeit, jederzeit die Werkseinstellung (wieder) in Kraft zu setzen.

⌧ Beim Abspeichern eines Konfigurations-Profils werden Passwörter nicht mitgespeichert.

Aktuelle Konfiguration als Konfigurations-Profil im mGuard speichern

1. In Feld *Name des neuen Profils* den gewünschten Namen eintragen
2. Die Schaltfläche **Speichere aktuelle Konfiguration als Profil** klicken.

Ein im mGuard gespeichertes Konfigurations-Profil anzeigen / aktivieren / löschen

Konfigurations-Profil anzeigen:

Den Namen des Konfigurations-Profils anklicken.

Konfigurations-Profil aktivieren:

Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Wiederherstellen** klicken.

Konfigurations-Profil löschen:

Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Löschen** klicken. Das Profil **Werkseinstellung** kann nicht gelöscht werden.

Konfigurations-Profil als Datei auf dem Konfigurationsrechner speichern

1. Rechts neben dem Namen des betreffenden Konfigurations-Profils die Schaltfläche **Download** klicken.
2. Legen Sie im angezeigten Dialogfeld den Dateinamen und Ordner fest, unter bzw. in dem das Konfigurations-Profil als Datei gespeichert wird. (Sie können die Datei beliebig benennen.)

Konfigurations-Profil vom Konfigurationsrechner auf den mGuard laden

Voraussetzung: Sie haben nach dem oben beschriebenem Verfahren ein Konfigurations-Profil als Datei auf dem Konfigurations-Rechners gespeichert.

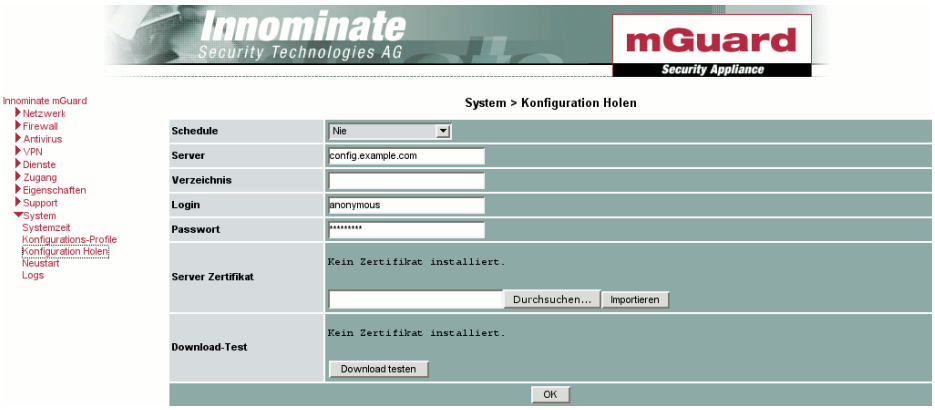
1. In Feld *Name des neuen Profils* den Namen eintragen, den das einzuladende Konfigurations-Profil erhalten soll.
2. Die Schaltfläche **Durchsuchen** klicken und dann die Datei selektieren.
3. Die Schaltfläche **Hochladen einer Konfiguration als Profil** klicken.

   Folge: Die hochgeladene Konfiguration erscheint in der Liste der Konfigurations-Profile.

Soll das hochgeladene Konfigurations-Profil aktiviert werden, klicken Sie neben dem Namen auf **Wiederherstellen.**

⌧ Wenn das Wiederherstellen einen Wechsel zwischen dem Stealth-Modus und einem der anderen Netzwerk-Modi beinhaltet, wird der mGuard neu gestartet.

System → Konfiguration holen



Der mGuard kann sich in einstellbaren Zeitintervallen eine neue Konfiguration von einem HTTPS Server holen. Wenn sich die neue Konfiguration von der aktuellen Konfiguration unterscheidet, wird diese automatisch aktiviert.

Schedule

Intervall, in welchem nach neuen Konfigurationen auf dem Server gesucht werden soll.

Server

IP oder Hostname des Servers, welcher die Konfigurationen bereitstellt.

Verzeichnis

Das Verzeichnis auf dem Server in dem die Konfiguration liegt.

Login

Login auf dem HTTPS Server.

Passwort

Passwort auf dem HTTPS Server.

Server Zertifikat

Das Zertifikat, welches den HTTPS Server, von dem die Konfiguration geholt wird, beglaubigt. Mit ihm soll verhindert werden, dass nicht authorisierte Konfigurationen auf dem mGuard installiert werden.

☞ Der Name der Konfigurationsdatei auf dem HTTPS Server ist die Seriennummer des mGuards inklusive der Endung „.atv“.

☞ Wenn die hinterlegten Konfigurationsprofile auch den privaten VPN Schlüssel für die VPN Verbindung oder VPN Verbindungen mit PSK enthalten:
Dann sollte das Passwort aus mindestens 30 zufälligen Groß- und Kleinbuchstaben, sowie Ziffern bestehen, um unerlaubten Zugriff auf diese zu verhindern.
Der HTTPS Server sollte weiterhin über den angegebenen Login nebst Passwort nur Zugriff auf die Konfiguration dieses einen mGuard ermöglichen. Ansonsten könnten sich die Nutzer anderer mGuards bzw. eines komprimitierten mGuards Zugriff auf diese anderen Konfigurationen verschaffen.

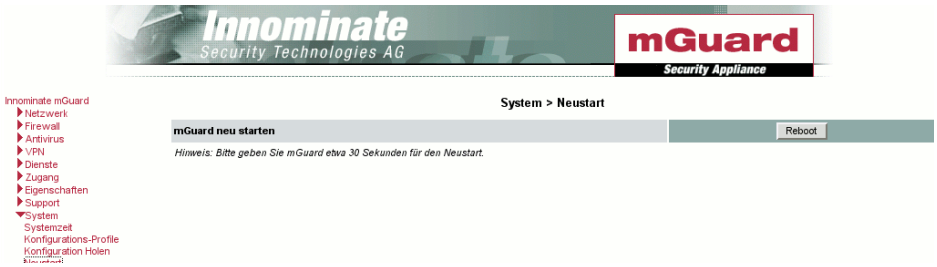
☞ Selbstunterschriebene Zertifikate (self-signed) sollten nicht die „key-usage“ Erweiterung verwenden.

Download-Test

Führt einen Test der angegebenen Parameter durch ohne diese zu speichern oder das gefunden Konfigurationsprofil zu aktivieren. Das Ergebnis des Tests erscheint anschließend auf der rechten Seite.

⌧ Sie sollten sicherstellen, dass das Profil auf dem Server keine unerwünschten mit „GAI_PULL_“ beginnenden Variablen enthält, welche die hier vorgenommene Konfiguration überschreiben.

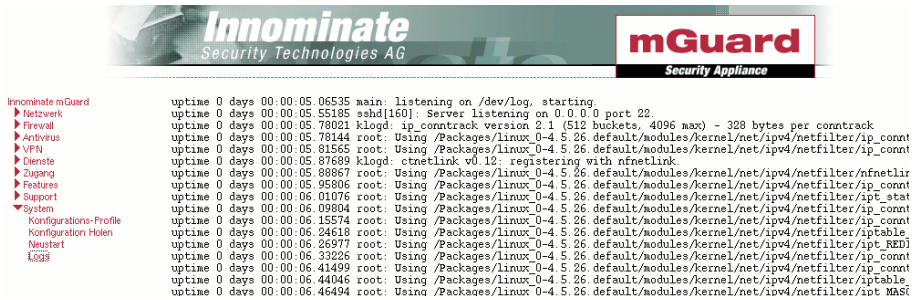
System → Neustart



Ein Neustart (= Reboot) ist erforderlich im Fehlerfall. Außerdem kann es erforderlich sein nach einem Software-Update.
Am Ende des Neustarts erscheint eine Meldung, dass man mit der Konfiguration fortfahren kann.
Ein Reboot kann auch durch aus- und wieder einschalten bewirkt werden.

System → Logs

Nur Anzeige


Innominate
Security Technologies AG
mGuard
Security Appliance
Innominate mGuard
Netzwerk
Firewall
Antivirus
VPN
Dienste
Zugang
Features
Support
System
Konfigurations-Profile
Konfiguration Holen
Neustart
Logs
uptime 0 days 00:00:05.06535 main: listening on /dev/log, starting.
uptime 0 days 00:00:05.55185 sshd[160]: Server listening on 0.0.0.0 port 22.
uptime 0 days 00:00:05.78021 klogd: ip_conntrack version 2.1 (512 buckets, 4096 max) - 328 bytes per conntrack
uptime 0 days 00:00:05.78144 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conn
uptime 0 days 00:00:05.81565 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conn
uptime 0 days 00:00:05.87689 klogd: ctnetlink v0.12: registering with nfnetlink.
uptime 0 days 00:00:05.88867 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/nfnetlin
uptime 0 days 00:00:05.95806 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conn
uptime 0 days 00:00:06.01076 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ipt_sta
uptime 0 days 00:00:06.09804 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conn
uptime 0 days 00:00:06.15574 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conn
uptime 0 days 00:00:06.24618 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/iptable_
uptime 0 days 00:00:06.26977 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ipt_RED
uptime 0 days 00:00:06.33226 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conn
uptime 0 days 00:00:06.41499 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ip_conn
uptime 0 days 00:00:06.44046 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/iptable_
uptime 0 days 00:00:06.46494 root: Using /Packages/linux_0-4.5.26.default/modules/kernel/net/ipv4/netfilter/ipt_MAS

Zeigt alle aufgezeichneten Log-Einträge (Gesamtlog).

Das Format entspricht dem unter Linux gebräuchlichen Format.

Es gibt spezielle Auswertungsprogramme, die Ihnen die Informationen aus den protokollierten Daten in einem besser lesbaren Format präsentieren.

Sie können die Log-Einträge auf einen externen Server übertragen. Siehe „Dienste → Remote Logging“ auf Seite 69.

5.15 CIDR (Classless InterDomain Routing)

IP Netzmasken und CIDR sind Notationen, die mehrere IP-Adressen zu einem Adressraum zusammenfassen. Dabei wird ein Bereich von aufeinanander folgenden Adressen als ein Netzwerk behandelt.

Um dem mGuard einen Bereich von IP-Adressen anzugeben, z. B. bei der Konfiguration der Firewall, kann es erforderlich sein, den Adressraum in der CIDR-Schreibweise anzugeben. Die nachfolgende Tabelle zeigt links die IP-Netzmaske, ganz rechts die entsprechende CIDR-Schreibweise.

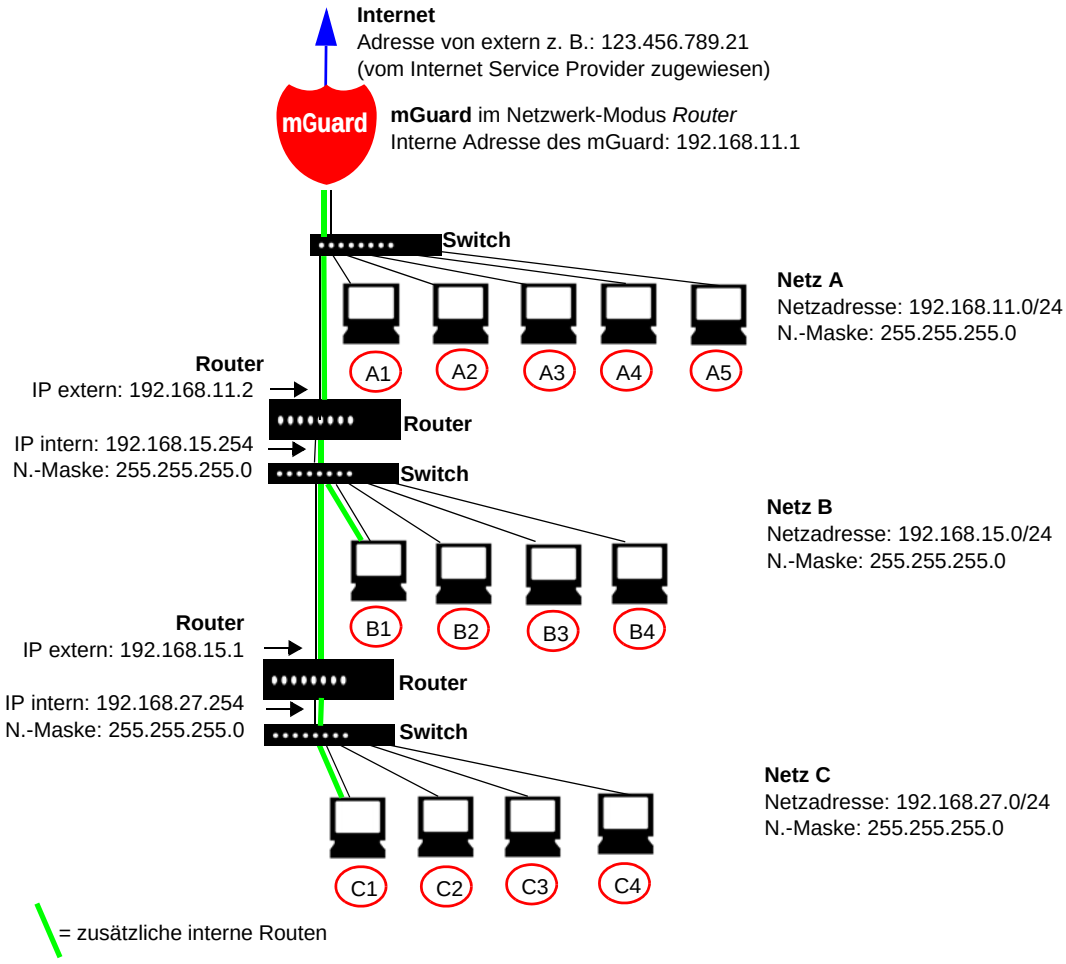
IP-Netzmaske	binär				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Beispiel: 192.168.1.0 / 255.255.255.0 entspricht im CIDR: 192.168.1.0/24

5.16 Netzwerk-Beispielskizze

Die nachfolgende Skizze zeigt, wie in einem lokalen Netzwerk mit Subnetzen die

IP-Adressen verteilt sein könnten, welche Netzwerk-Adressen daraus resultieren und wie die Angabe einer zusätzlichen internen Route lauten könnte.



Netz A

Rechner	A1	A2	A3	A4	A5
IP-Adresse	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Netz B

Rechner	B1	B2	B3	B4
IP-Adresse	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Netz C

Rechner	C1	C2	C3	C4
IP-Adresse	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4
Netzwerk-Maske	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Zusätzliche interne Routen:
Netzwerk: 192.168.15.0/24
Gateway: 192.168.11.2

Netzwerk: 192.168.27.0/24
Gateway: 192.168.11.2

6 Die Rescue-Taste für Neustart, Recovery-Prozedur und Flashen der Firmware

Die Rescue-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

6.1 Neustart durchführen

Ziel Das Gerät neu starten mit den konfigurierten Einstellungen.

Aktion: **Rescue-Taste** für ca. 1,5 Sekunden drückenODER

6.2 Recovery-Prozedur ausführen

Ziel Der mGuard soll in den Netzwerk-Modus (= Betriebsart) **Stealth** zurückgeschaltet werden, so dass er für Konfigurationszwecke wieder erreichbar ist unter folgender Adresse: **https://1.1.1.1/**

⌧ Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:
Der mGuard befindet sich im Router- oder PPPoE-Modus und
– die Geräteadresse des mGuard ist konfiguriert worden abweichend von der Standardeinstellung und
– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Aktion:
1. Die **Rescue-Taste** langsam 6-mal drücken.
2. Nach ca. 2 Sekunden antwortet der mGuard:
   - Bei Erfolg leuchtet die Status LED grün
   - Bei Mißerfolg bleibt die Status LED aus.
3. Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den *Stealth*-Modus. Es ist dann wieder unter folgender Adresse zu erreichen:
   https://1.1.1.1/

6.3 Flashen der Firmware

Ziel Die gesamte Software des mGuard soll neu ins Gerät geladen werden.

⌧ **Alle konfigurierten Einstellungen werden gelöscht.** Der mGuard wird in den Auslieferungszustand versetzt.

Mögliche Gründe zum Flashen der Firmware:
- Das Administrator- und Root-Passwort sind verloren gegangen.

Aktion: Gehen Sie wie folgt vor:

⌧ **Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die**

Stromversorgung des mGuard unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

Voraussetzungen:

- Sie haben die Software des mGuard von der mGuard-CD kopiert oder vom Innominate-Support bezogen und auf dem Konfigurations-Rechner gespeichert.
- DHCP- und TFTP-Server sind auf einem gemeinsamen Rechner installiert - siehe „Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server" auf Seite 92.

1. **Rescue-Taste** gedrückt halten, bis der *Recovery-Status* wie folgt eintritt:

   Der mGuard wird neu gestartet (nach ca. 1,5 Sekunden), nach weiteren ca. 1,5 Sekunden gelangt der mGuard in den *Recovery-Status*:

2. Spätestens 1 Sekunde nach Eintritt des *Recovery-Status* die **Rescue-Taste** loslassen.
   (Falls Sie die **Rescue-Taste** nicht loslassen, wird der mGuard neu gestartet.)
   Folge:
   Der mGuard startet das Recovery-System: Er sucht über die Schnittstelle für den lokal angeschlossenen Rechner bzw. das lokal angeschlossene Netzwerks nach dem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.
   - Statusanzeige: Die LED blinkt.
     Vom TFTP-Server wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur von Innominate unterschriebene Dateien werden geladen.
     Die Kontrollprozedur löscht nun den Flashspeicher und bereitet die Neuinstallation der Software vor.
   - Statusanzeige: Die bilden ein Lauflicht.
     Vom TFTP-Server die Software jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Innominate signierte Dateien werden akzeptiert.
     Dieser Vorgang dauert ca. 3 bis 5 Minuten.
   - Statusanzeige: Die mittlere LED (Heartbeart) leuchtet kontinuierlich.
     Die neue Software wird entpackt und konfiguriert. Das dauert ca. 5 Minuten. Sobald die Prozedur beendet ist, blinken durchgehend.

3. Starten Sie den mGuard neu.
   Drücken Sie dazu kurz die **Rescue-Taste**.
   ODER

   Folge:
   Der mGuard befindet sich im Auslieferungs-Zustand. Konfigurieren Sie ihn neu - siehe „Lokale Konfigurationsverbindung herstellen" auf Seite 12.

Voraussetzungen zum Flashen der Firmware: DHCP- und TFTP-Server

Zum „Flashen" der Firmware muss auf dem lokal angeschlossenen Rechner bzw. Netzwerk-Rechner ein DHCP- und TFTP-Server installiert sein.
(DHCP = **D**ynamic **H**ost **C**onfiguration **P**rotocol; TFTP = **T**rivial **F**ile **T**ransfer **P**rotocol)

Installieren Sie den DHCP- und TFTP-Server, falls notwendig (siehe unten).

⌦ Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden!

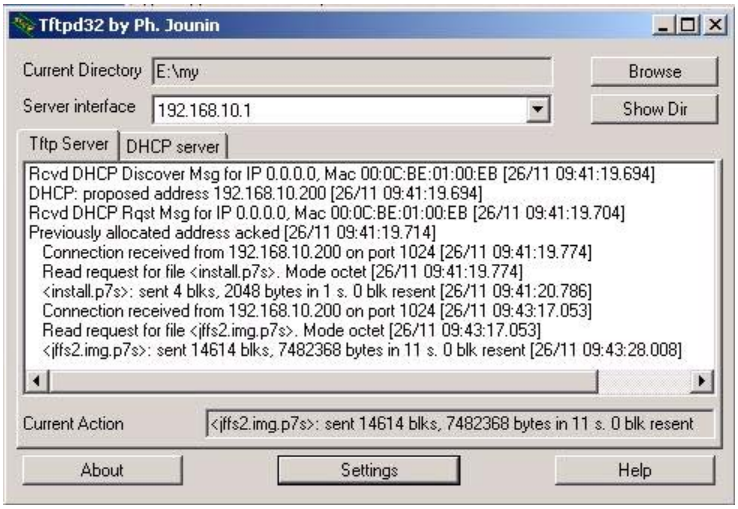
6.3.1 DHCP- und TFTP-Server unter Windows bzw. Linux installieren

Unter Windows:

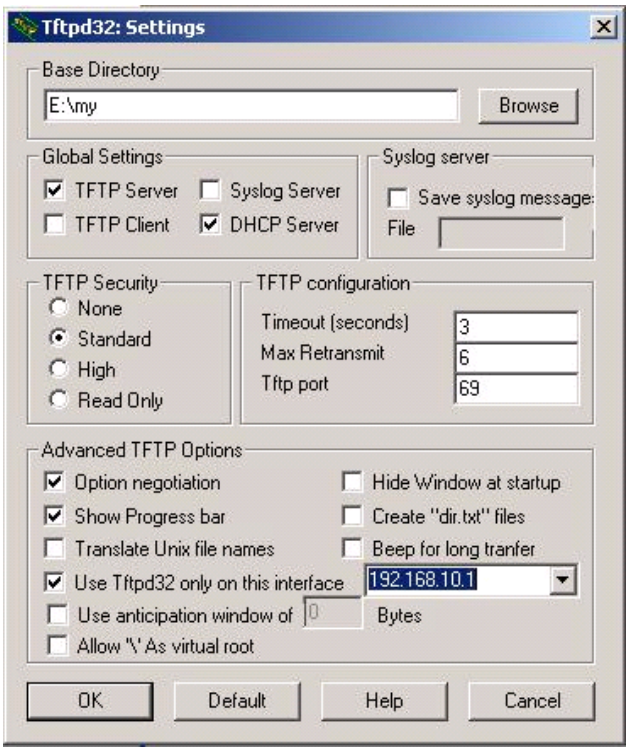
Installieren Sie das Programm, das sich auf der CD befindet. Gehen Sie dazu wie folgt vor:

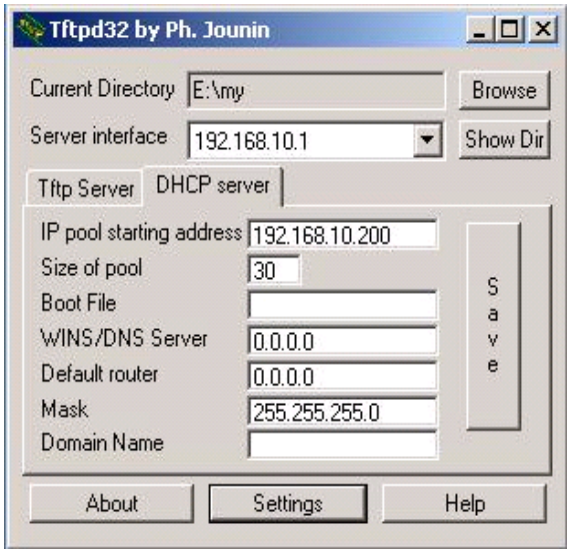
1. Ist der Windows-Rechner an einem Netzwerk angeschlossen, trennen Sie ihn von diesem.
2. Kopieren Sie die Software in einen beliebigen leeren Ordner des Windows-Rechners. Starten Sie das Programm TFTPD32.EXE
3. Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.
   Klicken Sie die Schaltfläche **Browse**, um auf den Ordner zu wechseln, wo die mGuard-Imagedateien gespeichert sind: *install.p7s, jffs2.img.p7s*

Die Image-Dateien befinden sich auch auf der CD, die zum Lieferumfang gehört.


Tftpd32 by Ph. Jounin
Current Directory E:\my
Browse
Server interface 192.168.10.1
Show Dir
Tftp Server
DHCP server
Rcvd DHCP Discover Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.694]
DHCP: proposed address 192.168.10.200 [26/11 09:41:19.694]
Rcvd DHCP Rqst Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.704]
Previously allocated address acked [26/11 09:41:19.714]
Connection received from 192.168.10.200 on port 1024 [26/11 09:41:19.774]
Read request for file <install.p7s>. Mode octet [26/11 09:41:19.774]
<install.p7s>: sent 4 blks, 2048 bytes in 1 s. 0 blk resent [26/11 09:41:20.786]
Connection received from 192.168.10.200 on port 1024 [26/11 09:43:17.053]
Read request for file <jffs2.img.p7s>. Mode octet [26/11 09:43:17.053]
<jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent [26/11 09:43:28.008]
Current Action
<jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent
About
Settings
Help

4. Wechseln Sie auf die Registerkarte Tftp Server bzw. DHCP Server und klikken Sie dann die Schaltfläche Settings, um im dann angezeigten Dialogfeld die Parameter wie folgt zu setzen:





Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server. Installieren Sie die entsprechenden Pakete gemäß der Anleitung der jeweiligen Distribution.
Konfigurieren Sie den DHCP-Server, indem Sie in der Datei **/etc/dhcp** folgende Einstellungen vornehmen:

```
subnet 192.168.134.0 netmask 255.255.255.0 {
range 192.168.134.100 192.168.134.119;
option routers 192.168.134.1;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.134.255;}
```

Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert:
/etc/inetd.conf
Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: **/tftpboot)**

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

Starten Sie dann den inetd-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
Sollten Sie einen anderen Mechanismus verwenden, z. B. xinetd, dann informieren Sie sich bitte in der entsprechenden Dokumentation.

7 Glossar

Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung werden Daten mit einem Schlüssel verschlüsselt und mit einem zweiten Schlüssel wieder entschlüsselt. Beide Schlüssel eignen sich zum Ver- und Entschlüsseln. Einer der Schlüssel wird von seinem Eigentümer geheim gehalten (Privater Schlüssel/Private Key), der andere wird der Öffentlichkeit (Öffentlicher Schlüssel/Public Key), d. h. möglichen Kommunikationspartnern, gegeben.
Eine mit dem öffentlichen Schlüssel verschlüsselte Nachricht kann nur von dem Empfänger entschlüsselt und gelesen werden, der den zugehörigen privaten Schlüssel hat. Eine mit dem privaten Schlüssel verschlüsselte Nachricht kann von jedem Empfänger entschlüsselt werden, der den zugehörigen öffentlichen Schlüssel hat. Die Verschlüsselung mit dem privaten Schlüssel zeigt, daß die Nachricht tatsächlich vom Eigentümer des zugehörigen öffentlichen Schlüssels stammt. Daher spricht man auch von digitaler Signatur, Unterschrift.
Assymetrische Verschlüsselungsverfahren wie RSA sind jedoch langsam und anfällig für bestimmte Angriffe, weshalb sie oft mit einem symmetrischen Verfahren kombiniert werden (→ symmetrische Verschlüsselung). Andererseits sind Konzepte möglich, die die aufwendige Administrierbarkeit von symmetrischen Schlüsseln vermeiden.

DES / 3DES

Der von IBM stammende und von der NSA überprüfte symmetrische Verschlüsselungsalgorithmus (→ symmetrische Verschlüsselung) DES wurde 1977 vom amerikanischen National Bureau of Standards, dem Vorgänger des heutigen National Institute of Standards and Technology (NIST), als Standard für amerikanische Regierungsinstitutionen festgelegt. Das es sich hierbei um den ersten standardisierten Verschlüsslungsalgorithmus überhaupt handelte, setzte er sich auch schnell in der Industrie und somit außerhalb Amerikas durch.
DES arbeitet mit einer Schlüssellänge von 56Bit, die heute aufgrund der seit 1977 gestiegenen Rechenleistung der Computer als nicht mehr sicher gilt.
3DES ist eine Variante von DES. Es arbeitet mit 3 mal größeren Schlüsseln, die also 168 Bit lang sind. Sie gilt heute noch als sicher und ist unter anderem auch Teil des IPsec-Standards.

AES

Das NIST (National Institute of Standards and Technology) entwickelt in Zusammenarbeit mit Industrie-Unternehmen seit Jahren den AES-Verschlüsselungsstandard. Diese → symmetrische Verschlüsselung soll den bisherigen DES-Standard ablösen. Der AES-Standard spezifiziert drei verschiedene Schlüsselgrößen mit 128, 192 und 256 Bit.
1997 hatte die NIST die Initiative zu AES gestartet und ihre Bedingungen für den Algorithmus bekannt gegeben. Von den vorgeschlagenen Verschlüsselungsalgorithmen hat die NIST fünf Algorithmen in die engere Wahl gezogen; und zwar die Algorithmen MARS, RC6, Rijndael, Serpent und Twofish. Im Oktober 2000 hat man sich für Rijndael als Verschlüsselungsalgorithmus entschieden.

Client / Server

In einer Client-Server-Umgebung ist ein Server ein Programm oder Rechner, das vom Client-Programm oder Client-Rechner Anfragen entgegennimmt und beantwortet.
Bei Datenkommunikation bezeichnet man auch den Rechner als Client, der eine Verbindung zu einem Server (oder Host) herstellt. D. h. der Client ist der anrufende Rechner, der Server (oder Host) der angerufene.

Datagramm

Bei IP Übertragungsprotokollen werden Daten in Form von Datenpaketen, den sog. IP-Datagrammen, versendet. Ein IP-Datagramm hat folgenden Aufbau:

IP-Header	TCP, UDP, ESP etc. Header	Daten (Payload)

Der IP-Header enthält:
– die IP-Adresse des Absenders (source IP-address)
– die IP-Adresse des Empfängers (destination IP-adress)
– die Protokollnummer des Protokoll der nächst höheren Protokollschicht (nach dem OSI-Schichtenmodell)
– die IP-Header Prüfsumme (Checksum) zur Überprüfung der Integrität des Headers beim Empfang.

Der TCP-/UDP-Header enthält folgende Informationen:
– Port des Absenders (source port)
– Port des Empfängers (destination port)
– eine Prüfsume über den TCP-Header und ein paar Informationen aus dem IP-Header (u. a. Quell- und Ziel-IP-Adresse)

DynDNS-Anbieter

Auch *Dynamic DNS-Anbieter*. Jeder Rechner, der mit dem Internet verbunden ist, hat eine IP-Adresse (IP = Internet Protocol) Eine IP-Adresse besteht aus 4 maximal dreistelligen Nummern, jeweils durch einem Punkt getrennt. Ist der Rechner über die Telefonleitung per Modem, per ISDN oder auch per ADSL online, wird ihm vom Internet Service Provider dynamisch eine IP-Adresse zugeordnet, d. h. die Adresse wechselt von Sitzung zu Sitzung. Auch wenn der Rechner (z. B. bei einer Flatrate) über 24 Stunden ununterbrochen online ist, wird die IP-Adresse zwischendurch gewechselt.
Soll ein lokaler Rechner über das Internet erreichbar sein, muss er eine Adresse haben, die der entfernten Gegenstelle bekannt sein muss. Nur so kann diese die Verbindung zum lokalen Rechner aufbauen. Wenn die Adresse des lokalen Rechners aber ständig wechselt, ist das nicht möglich. Es sei denn, der Betreiber des lokalen Rechners hat ein Account bei einem DynamicDNS-Anbieter (DNS = Domain Name Server).
Dann kann er bei diesem einen Hostnamen festlegen, unter dem der Rechner künftig erreichbar sein soll, z. B.: www.example.com. Zudem stellt der DynamicDNS-Anbieter ein kleines Programm zur Verfügung, das auf dem betreffenden Rechner installiert und ausgeführt werden muss. Bei jeder Internet-Sitzung des lokalen Rechners teilt dieses Tool dem DynamicDNS-Anbieter mit, welche IP-Adresse der Rechner zurzeit hat. Dessen Domain Name Server registriert die aktuelle Zuordnung Hostname - IP-Adresse und teilt diese anderen Domain Name Servern im Internet mit.
Wenn jetzt ein entfernte Rechner eine Verbindung herstellen will zum lokalen Rechner, der beim DynamicDNS-Anbieter registriert ist, benutzt der entfernte Rechner den Hostnamen des lokalen Rechners als Adresse. Dadurch wird eine Verbindung hergestellt zum zuständigen DNS (Domain Name Server), um dort die IP-Adresse nachzuschlagen, die diesem Hostnamen zurzeit zugeordnet ist. Die IP-Adresse wird zurückübertragen zum entfernten Rechner und jetzt von diesem als Zieladresse benutzt. Diese führt jetzt genau zum gewünschten lokalen Rechner.
Allen Internetadressen liegt im Grunde dieses Verfahren zu Grunde: Zunächst wird eine Verbindung zum DNS hergestellt, um die diesem Hostnamen zugeteilte IP-Adresse zu ermitteln. Ist das geschehen, wird mit dieser „nachgeschlagenen“ IP-Adresse die Verbindung zur gewünschten Gegenstelle, eine beliebige Internetpräsenz, aufgebaut.

IP-Adresse

Jeder Host oder Router im Internet / Intranet hat eine eindeutige IP-Adresse (IP = Internet Protocol). Die IP-Adresse ist 32 Bit (= 4 Byte) lang und wird geschrieben als 4 Zahlen (jeweils im Bereich 0 bis 255), die durch einen Punkt voneinander getrennt sind.
Eine IP-Adresse besteht aus 2 Teilen: die Netzwerk-Adresse und die Host-Adresse.

Netzwerk-Adresse	Host-Adresse

Alle Hosts eines Netzes haben dieselbe Netzwerk-Adresse, aber unterschiedliche Host-Adressen. Je nach Größe des jeweiligen Netzes - man unterscheidet Netze der Kategorie Class A, B und C - sind die beiden Adressanteile unterschiedlich groß:

	1. Byte	**2. Byte**	**3. Byte**	**4. Byte**
Class A	Netz-Adr.	Host-Adr.		
Class B	Netz-Adr.		Host-Adr.	
Class C	Netz-Adr.			Host-Adr.

Ob eine IP-Adresse ein Gerät in einem Netz der Kategorie Class A, B oder C bezeichnet, ist am ersten Byte der IP-Adresse erkennbar. Folgendes ist festgelegt:

	Wert des 1. Byte	**Bytes für die Netzadresse**	**Bytes für die Host-Adresse**
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Rein rechnerisch kann es nur maximal 126 Class A Netze auf der Welt geben, jedes dieser Netze kann maximal 256 x 256 x 256 Hosts umfassen (3 Bytes Adressraum). Class B Netze können 64 x 256 mal vorkommen und können jeweils bis zu 65.536 Hosts enthalten (2 Bytes Adressraum: 256 x 256). Class C Netze können 32 x 256 x 256 mal vorkommen und können jeweils bis zu 256 Hosts enthalten (1 Byte Adressraum).

Subnetz-Maske

Einem Unternehmens-Netzwerk mit Zugang zum Internet wird normalerweise nur eine einzige IP-Adresse offiziell zugeteilt, z. B. 123.456.789.21. Bei dieser Beispiel-Adresse ist am 1. Byte erkennbar, dass es sich bei diesem Unternehmens-Netzwerk um ein Class B Netz handelt, d. h. die letzten 2 Byte können frei zur Host-Adressierung verwendet werden. Das ergibt rein rechnerisch einen Adressraum von 65.536 möglichen Hosts (256 x 256).
Ein so riesiges Netz macht wenig Sinn. Hier entsteht der Bedarf, Subnetze zu bilden. Dazu dient die Subnetz-Maske. Diese ist wie eine IP-Adresse ein 4 Byte langes Feld. Den Bytes, die die Netz-Adresse repräsentieren, ist jeweils der Wert 255 zugewiesen. Das dient vor allem dazu, sich aus dem Host-Adressenbereich einen Teil zu „borgen“, um diesen zur Adressierung von Subnetzen zu benutzen. So kann beim Class B Netz (2 Byte für Netzwerk-Adresse, 2 Byte für Host-Adresse) mit Hilfe der Subnetz-Maske 255.255.255.0 das 3. Byte, das eigentlich für Host-Adressierung vorgesehen war, jetzt für Subnetz-Adressierung verwen-

det werden. Rein rechnerisch können so 256 Subnetze mit jeweils 256 Hosts entstehen.

IPsec

IP Security (IPsec) ist ein Standard, der es ermöglicht, bei IP-Datagrammen (→ Datagramm) die Authentizität des Absenders, die Vertraulichkeit und die Integrität der Daten durch Verschlüsselung zu wahren. Die Bestandteile von IPsec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die Security Association (SA) und der Internet Key Exchange (IKE).
Zu Beginn der Kommunikation klären die an der Kommunikation beteiligten Rechner das benutzte Verfahren und dessen Implikationen wie z. B. *Transport Mode* oder *Tunnel Mode*
Im *Transport Mode* wird in jedes IP-Datagramm zwischen IP-Header und TCP- bzw. UDP-Header ein IPsec-Header eingesetzt. Da dadurch der IP-Header unverändert bleibt, ist dieser Modus nur für eine Host- zu-Host-Verbindung geeignet.
Im *Tunnel Mode* wird dem gesamten IP-Datagramm ein IPsec-Header und ein neuer IP-Header vorangestellt. D. h. das ursprüngliche Datagramm wird insgesamt verschlüsselt in der Payload des neuen Datagramms untergebracht.
Der *Tunnel Mode* findet beim VPN Anwendung: Die Geräte an den Tunnelenden sorgen für die Ver- bzw. Entschlüsselung der Datagramme, auf der Tunnelstrekke, d. h. auf dem Übertragungsweg über ein öffentliches Netz bleiben die eigentlichen Datagramme vollständig geschützt.

NAT (Network Address Translation)

Bei der Network Address Translation (NAT) - oft auch als *IP-Masquerading* bezeichnet - wird hinter einem einzigen Gerät, dem sog. NAT-Router, ein ganzes Netzwerk „versteckt“. Die internen Rechner im lokalen Netz bleiben mit ihren IP-Adressen verborgen, wenn Sie nach außen über die NAT-Router kommunizieren. Für die Kommunikationspartner außen erscheint nur der NAT-Router mit seiner eigenen IP-Adresse.
Damit interne Rechner dennoch direkt mit externen Rechnern (im Internet) kommunizieren können, muss der NAT-Router die IP-Datagramme verändern, die von internen Rechnern nach außen und von außen zu einem internen Rechner gehen.
Wird ein IP-Datagramm aus dem internen Netz nach außen versendet, verändert der NAT-Router den UDP- bzw. TCP-Header des Datagramms. Er tauscht die Quell-IP-Adresse und den Quell-Port aus gegen die eigene offizielle IP-Adresse und einen eigenen, bisher unbenutzen Port. Dazu führt er eine Tabelle, die die Zuordnung der ursprünglichen mit den neuen Werten herstellt.
Beim Empfang eines Antwort-Datagramms erkennt der NAT-Router anhand des angegebenen Zielports, dass das Datagramm eigentlich für einen internen Rechner bestimmt ist. Mit Hilfe der Tabelle tauscht der NAT-Router die Ziel-IP-Adresse und den Ziel-Port aus und schickt das Datagramm weiter ins interne Netz.

Port-Nummer

Bei den Protokollen UDP und TCP wird jedem Teilnehmer eine Portnummer zugeordnet. Über sie ist es möglich zwischen zwei Rechnern mehrere UDP oder TCP Verbindungen zu unterscheiden und somit gleichzeitig zu nutzen.
Bestimmte Portnummern sind für spezielle Zwecke reserviert. Zum Beispiel werden in der Regel HTTP Verbindungen zu TCP Port 80 oder POP3 Verbindungen zu TCP Port 110 aufgebaut.

PPPoE

Akronym für **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. Basiert auf den Standards PPP und Ethernet. PPPoE ist eine Spezifikation, um Benutzer per Ethernet mit dem Internet zu verbinden über ein gemeinsam benutztes Breitbandmedium wie

DSL, Wireless LAN oder Kabel-Modem.

PPTP

Akronym für **P**oint-to-**P**oint **T**unneling **P**rotocol. Entwickelt von Microsoft, U.S. Robotics und anderen wurde dieses Protokoll entwickelt, um zwischen zwei VPN-Knoten (→ VPN) über ein öffentliches Netz sicher Daten zu übertragen.

X.509 Zertifikat

Eine Art „Siegel“, welches die Echtheit eines öffentlichen Schlüssels (→ asymmetrische Verschlüsselung) und zugehöriger Daten belegt.

Damit der Benutzer eines zum Verschlüsseln dienenden öffentlichen Schlüssels sichergehen kann, dass der ihm übermittelte öffentliche Schlüssel wirklich von seinem tatsächlichen Aussteller und damit der Instanz stammt, die die zu versendenden Daten erhalten soll, gibt es die Möglichkeit der Zertifizierung. Diese Beglaubigung der Echtheit des öffentlichen Schlüssels und die damit verbundene Verknüpfung der Identität des Ausstellers mit seinem Schlüssel übernimmt eine zertifizierende Stelle (*Certification Authority - CA*). Dies geschieht nach den Regeln der CA, indem der Aussteller des öffentlichen Schlüssels beispielsweise persönlich zu erscheinen hat. Nach erfolgreicher Überprüfung signiert die CA den öffentliche Schlüssel mit ihrer (digitalen) Unterschrift, ihrer Signatur. Es entsteht ein Zertifikat.

Ein X.509(v3) Zertifikat beinhaltet also einen öffentlichen Schlüssel, Informationen über den Schlüsseleigentümer (angegeben als Distinguised Name (DN)), erlaubte Verwendungszwecke usw. und die Signatur der CA.

Die Signatur entsteht wie folgt: Aus der Bitfolge des öffentlichen Schlüssels, den Daten über seinen Inhaber und aus weiteren Daten erzeugt die CA eine individuelle Bitfolge, die bis zu 160 Bit lang sein kann, den sog. HASH-Wert. Diesen verschlüsselt die CA mit ihrem privaten Schlüssel und fügt ihn dem Zertifikat hinzu. Durch die Verschlüsselung mit dem privaten Schlüssel der CA ist die Echtheit belegt, d. h. die verschlüsselte HASH-Zeichenfolge ist die digitale Unterschrift der CA, ihre Signatur. Sollten die Daten des Zertifikats missbräuchlich geändert werden, stimmt dieser HASH-Wert nicht mehr, das Zertifikat ist dann wertlos.

Der HASH-Wert wird auch als Fingerabdruck bezeichnet. Da er mit dem privaten Schlüssel der CA verschlüsselt ist, kann jeder, der den zugehörigen öffentlichen Schlüssel besitzt, die Bitfolge entschlüsseln und damit die Echtheit dieses Fingerabdrucks bzw. dieser Unterschrift überprüfen.

Durch die Heranziehung von Beglaubigungsstellen ist es möglich, dass nicht jeder Schlüsseleigentümer den anderen kennen muss, sondern nur die benutzte Beglaubigungsstelle. Die zusätzlichen Informationen zu dem Schlüssel vereinfachen zudem die Administrierbarkeit des Schlüssels.

X.509 Zertifikate kommen z.B. bei Email Verschlüsselung mittels S/MIME oder IPsec zum Einsatz.

Protokoll, Übertragungsprotokoll

Geräte, die miteinander kommunizieren, müssen dieselben Regeln dazu verwenden. Sie müssen dieselbe „Sprache sprechen“. Solche Regeln und Standards bezeichnet man als Protokoll bzw. Übertragungsprotokoll. Oft benutze Protokolle sind z. B. IP, TCP, PPP, HTTP oder SMTP.

Service Provider

Anbieter, Firma, Institution, die Nutzern den Zugang zum Internet oder zu einem Online-Dienst verschafft.

Spoofing, Antispoofing

In der Internet-Terminologie bedeutet Spoofing die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein.

Unter Anti-Spoofing versteht man Mechanismen, die Spoofing entdecken oder verhindern.

Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung werden Daten mit dem gleichen Schlüssel ver- und entschlüsselt. Beispiele für symmetrische Verschlüsselungsalgorithmen sind DES und AES. Sie sind schnell, jedoch bei steigender Nutzerzahl nur aufwendig administrierbar.

TCP/IP (Transmission Control Protocol/ Internet Protocol)

Netzwerkprotokolle, die für die Verbindung zweier Rechner im Internet verwendet werden.
IP ist das Basisprotokoll.
UDP baut auf IP auf und verschickt einzelne Pakete. Diese können beim Empfänger in einer anderen Reihenfolge als der abgeschickten ankommen, oder sie können sogar verloren gehen.
TCP dient zur Sicherung der Verbindung und sorgt beispielsweise dafür, dass die Datenpakete in der richtigen Reihenfolge an die Anwendung weitergegeben werden.
UDP und TCP bringen zusätzlich zu den IP-Adressen Port-Nummern zwischen 1 und 65535 mit, über die die unterschiedlichen Dienste unterschieden werden.
Auf UDP und TCP bauen eine Reihe weiterer Protokolle auf, z. B. HTTP (Hyper Text Transfer Protokoll), HTTPS (Secure Hyper Text Transfer Protokoll), SMTP (Simple Mail Transfer Protokoll), POP3 (Post Office Protokoll, Version 3), DNS (Domain Name Service).
ICMP baut auf IP auf und enthält Kontrollnachrichten.
SMTP ist ein auf TCP basierendes E-Mail-Protokoll.
IKE ist ein auf UDP basierendes IPsec-Protokoll.
ESP ist ein auf IP basierendes IPsec-Protokoll.
Auf einem Windows-PC übernimmt die WINSOCK.DLL (oder WSOCK32.DLL) die Abwicklung der beiden Protokolle.
(→ Datagramm)

VLAN

Über ein VLAN (Virtual Local Area Network) kann man ein physikalisches Netzwerk logisch in getrennte, nebeneinander existierende Netze unterteilen. Die Geräte der unterschiedlichen VLANs können dabei nur Geräte in ihrem eigenen VLAN erreichen. Die Zuordnung zu einem VLAN wird damit nicht mehr nur allein von der Topologie des Netzes bestimmt, sondern auch durch die konfigurierte VLAN ID.

Die VLAN Einstellung kann als optionale Einstellung zu jeder IP vorgenommen werden. Ein VLAN wird dabei durch seine VLAN ID (1-4094) identifiziert. Alle Geräte mit der selben VLAN ID gehören dem gleichen VLAN an und können miteinander kommunizieren.
Das Ethernet-Paket wird für VLAN nach IEEE 802.1Q um 4 Byte erweitert, davon stehen 12 Bit zur Aufnahme der VLAN ID zur Verfügung. Die VLAN ID „0“ und „4095“ sind reserviert und nicht zur Identifikation eines VLANs nutzbar.

VPN (Virtuelles Privates Netzwerk)

Ein **V**irtuelles **P**rivates **N**etzwerk (VPN) schließt mehrere voneinander getrennte private Netzwerke (Teilnetze) über ein öffentliches Netz, z. B. das Internet, zu einem gemeinsamen Netzwerk zusammen. Durch Verwendung kryptographischer Protokolle wird dabei die Vertraulichkeit und Authentizität gewahrt. Ein VPN bietet somit eine kostengünstige Alternative gegenüber Standleitungen, wenn es darum geht, ein überregionales Firmennetz aufzubauen.

8 Technische Daten

CPU	Intel IXP 42x mit 266 MHz (bzw. 533 MHz mGuard delta enterprise XL)
Speicher	16 MB Flash, 64 MB SDRAM
LAN u. WAN Schnittstellen	Ethernet IEEE 802 10/100 Mbps (4 LAN, 1 WAN) RJ45
Seriell	RS 232
Stromversorgung	5V DC, 3A
Betriebssystem	Innominate Embedded Linux
Funktionsüberwachung	Watchdog und optische Anzeige
Relative Luftfeuchtigkeit	5-95% (nicht kondensierend)
Umgebungstemperatur	-20° bis 70°C

Notes on CE identification

This device comply with the regulations of the following European directive: 89/336/EEC Council Directive on the harmonization of the legal regulations of member states on electromagnetic compatibility (amended by Directives 91/263/EEC, 92/31/EEC and 93/68/EEC).

The EU declaration of conformity is kept available for the responsible authorities in accordance with the above-mentioned EU directives at:

Innominate Security Technologies AG
Albert-Einstein-Str. 14
D-12489 Berlin
Telephone ++49 (0)30 6392-3300

The product can be used in the residential sphere (residential sphere, business and trade sphere and small companies) and in the industrial sphere.

- Interference proof:
  EN 61000-6-2:2001
- Emitted immunity:
  EN 55022:1998
  + A1 2000
  + A2 2003, Class A

FCC Note

This equipment has been tested and found to comply with the limits for a Class A digital device, persuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the

equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.